telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

March 2022

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 predictable monthly fee.

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

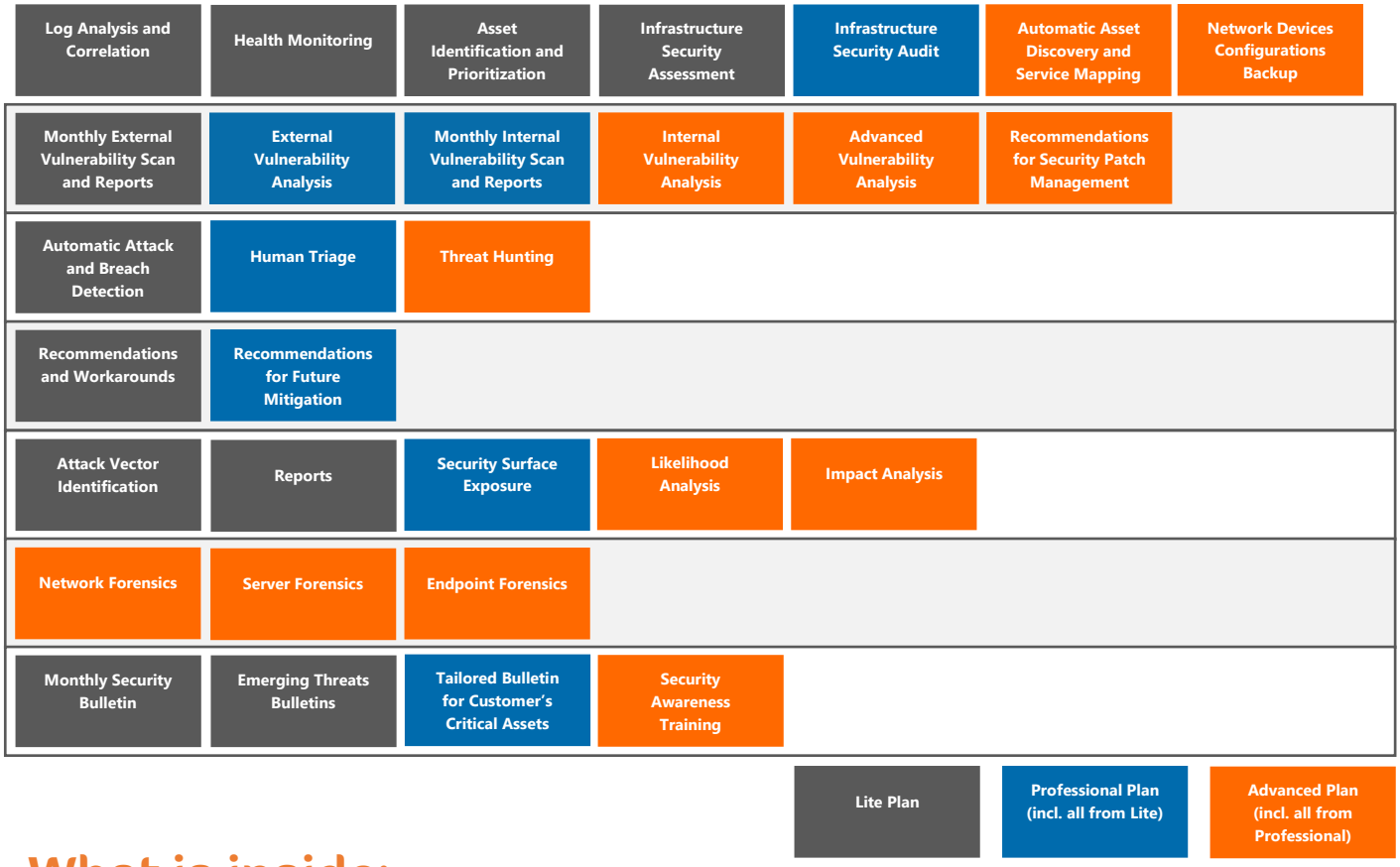
Start to mitigate cyber threats and minimize the risk!

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!



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. German petrol supply firm Oiltanking paralyzed by cyber attack

Oiltanking GmbH, a German petrol distributor who supplies Shell gas stations in the country, has fallen victim to a cyberattack that severely impacted its operations.

Additionally, the attack has also affected Mabanaft GmbH, an oil supplier. Both entities are subsidiaries of the Marquard & Bahls group, which may have been the breach point.

Supply stable but volatile

Because the firm supplies a total of 26 companies in the country with fuel, German media raised worries about shortages immediately, but officials came forth to appease them.

Shell alone operates 1,955 gas stations in the country, so if they were to run out of fuel, it would cause a crisis that would have an adverse effect on an array of Germany's day-to-day operations, and by extension its national economy.

The managing director of the independent tank storage association in Germany, Frank Shaper, told Spiegel that the attack does not endanger the supply of fuel in the country neither on heating nor the transportation aspects.

However, the disruption remains significant, and if it takes the firm a long time to resolve the IT problems caused by the attack, the supply chain could also be disrupted.

This is mainly due to the automation of the tank loading/unloading process that cannot fall back to manual operations since it relies entirely on computerized systems that are currently offline.

Oiltanking operates a total of 13 tank farms in Germany, and currently, these cannot serve trucks. Instead, the firm has resorted to using alternative charging points until the effects of the cyberattack are remediated.

Bleeping Computer received the following comment from the company regarding the current situation:

> *On Saturday, January 29th 2022, Oiltanking GmbH Group and Mabanaft GmbH & Co. KG (Mabanaft) Group discovered we have been the victim of a cyber incident affecting our IT systems. Upon learning of the incident, we immediately took steps to enhance the security of our systems and processes and launched an investigation into the matter. We are working to solve this issue according to our contingency plans, as well as to understand the full scope of the incident. We are undertaking a thorough investigation, together with external specialists and are collaborating closely with the relevant authorities. All terminals continue to operate safely.*
>
> *Oiltanking Deutschland GmbH & Co. KG, an operating unit within the Mabanaft Group, operates all terminals in Germany and is not part of the Oiltanking GmbH Group.*

> *Oiltanking GmbH Group continues to operate all terminals in all global markets. Oiltanking Deutschland GmbH & Co. KG terminals are operating with limited capacity and have declared force majeure. Mabanaft Deutschland GmbH & Co. KG has also declared force majeure for the majority of its inland supply activities in Germany. All parties continue to work to restore operations to normal in all our terminals as soon as possible.*

Last week, the German intelligence service, BfV, warned local firms of ongoing cyberattacks coordinated by the APT27 Chinese state-supported hacking group.

While the attack on Oiltanking hasn't been attributed to any actors yet, it could be the work of a state actor who seeks to cause large-scale disruption and economic damage.

Source: https://www.bleepingcomputer.com/news/security/german-petrol-supply-firm-oiltanking-paralyzed-by-cyber-attack/

2. Telco fined €9 million for hiding cyberattack impact from customers

The Greek data protection authority has imposed fines of 5,850,000 EUR ($6.55 million) to COSMOTE and 3,250,000 EUR ($3.65 million) to OTE, for leaking sensitive customer communication due to a cyberattack.

As the agency says in an announcement, COSMOTE infringed at least eight articles of the GDPR, including violating its duty to inform affected customers of the true impact of the incident.

OTE (Hellenic Telecommunications Organization) and COSMOTE belong to the same entity, OTE Group, which is the largest technology company in Greece, offering fixed and mobile telephony, broadband, and network communication services.

The hacking incident

An internal investigation conducted by COSMOTE in 2020 revealed that a hacker social engineered one of its employees through LinkedIn and later used brute-forcing tools to derive the target's account credentials.

According to the findings of the investigation, the adversary used a Lithuanian IP address for accessing one of OTE's servers repeatedly.

The threat actor leveraged the account credentials to steal database files on five separate occasions. The size of the stolen data amounted to 48GB.

COSMOTE keeps call details on its servers for 90 days for service quality assurance, and maintains an anonymized version of the data for another 12 months for statistical analysis that helps in targeted service improvement.

As the data protection authority probe discovered, the anonymization process wasn't properly done, and the data holding periods weren't strictly respected.

The impact

The compromised server contained sensitive subscriber details and call data that concerned the period between September 1, 2020, and September 5, 2020.

More specifically, the exposed details include the following:

- Rough positional data of 4,792,869 unique COSMOTE subscribers.
- Age, gender, plan, and ARPU of 4,239,213 unique COSMOTE subscribers.
- MSISDN/CLI of 6,939,656 users of other telecommunication providers who communicated with customers of COSMOTE.
- MSISDN, IMEI, IMSI, and connected tower position for 281,403 roaming subscribers of COSMOTE.

The above information could be used for highly targeted social engineering, phishing, and even extortion in some cases.

Still, the impact of the hacking incident could be significant for targeted subscribers who may be high-interest individuals.

Source: https://www.bleepingcomputer.com/news/security/telco-fined-9-million-for-hiding-cyberattack-impact-from-customers/

3. Charming Kitten Sharpens Its Claws with PowerShell Backdoor

The notorious Iranian APT is fortifying its arsenal with new malicious tools and evasion tactics and may even be behind the Memento ransomware.

The Iranian advanced persistent threat (APT) Charming Kitten is sharpening its claws with a new set of tools, including a novel PowerShell backdoor and related stealth tactics, that show the group evolving yet again. The new tools may signal that it's getting ready to pounce on new victims, researchers believe.

Researchers at cybersecurity firm Cybereason discovered the tools, which include a backdoor they dubbed "PowerLess Backdoor," as well as an evasive maneuver to run the backdoor in a .NET context rather than as one that triggers a PowerShell process, the Cybereason Nocturnus Team wrote in a report published Tuesday.

"The Cybereason Nocturnus Team was able to identify a new toolset that includes a novel backdoor, malware loaders, a browser info stealer, and a keylogger," Cybereason Senior Malware Researcher Daniel Frank wrote in the report.

The team also identified links between Charming Kitten and the Memento ransomware that emerged late last year and until now has been unattributed, signaling that the APT may be moving beyond its typical cyberespionage tactics and into new cybercriminal territory, researchers said.

Charming Kitten is a prolific APT believed to be backed by the Iranian government and known by a number of other names – including TA453, APT35, Ajax Security Team, NewsBeef, Newscaster and Phosphorus.

The group – which first rose to prominence in 2018 – was extremely active throughout 2020 and 2021 and is best known for targeted cyber-espionage attacks against politicians, journalists, human-rights activists, researchers, scholars and think tanks.

Some of the APT's more high-profile attacks occurred in 2020, when the group targeted the Trump and Biden presidential campaigns as well as attendees of two global geo-political summits, the Munich Security Conference and the Think 20 (T20) Summit, in separate and various incidents.

New Quiver of Malware

The Cybereason Nocturnus team uncovered a raft of new Charming Kitten activity when they investigated threat-intelligence efforts that "included pivoting on an IP address (162.55.136[.]20) that was already attributed to Iranian threat actors by multiple sources, including US CERT," Frank explained.

The team took a deeper dive into different files that were downloaded from the IP address and discovered a treasure trove of novel tools as well as links to Memento ransomware, he said.

Charming Kitten is now using what researchers have dubbed PowerLess Backdoor, a previously undocumented PowerShell trojan that supports downloading additional payloads, such as a keylogger and an info stealer.

The team also discovered a unique new PowerShell execution process related to the backdoor aimed at slipping past security-detection products, Frank wrote.

"The PowerShell code runs in the context of a .NET application, thus not launching 'powershell.exe' which enables it to evade security products," he wrote.

Overall, the new tools show Charming Kitten developing more "modular, multi-staged malware" with payload-delivery aimed at "both stealth and efficacy," Frank noted. The group also is leaning heavily on open-source tools such as cryptography libraries, weaponizing them for payloads and communication encryption, he said.

This reliance on open-source tools demonstrates that the APT's developers likely lack "specialization in any specific coding language" and possess "intermediate coding skills," Frank observed.

The Memento Connection

Cybereason Nocturnus also found that another IP that US CERT has linked to Charming Kitten,91.214.124[.]143, has been communicating with malicious files and has "unique URL directory patterns that reveal a potential connection to Memento ransomware," Frank wrote.

"The string 'gsdhdDdfgA5sS' appears to be generated by the same script as the one listed in the Memento ransomware IOCs – "gadfTs55sghsSSS" – he explained, citing specific directory activity that researchers observed. "The domain 'google.onedriver-srv[.]ml' was previously resolved to the IP address 91.214.124[.]143 mentioned in the US CERT alert about Iran state-sponsored actors activity."

Analyzing this directory activity points to the IP potentially serving as a domain being used as command and control (C2) for Memento, researchers found.

Indeed, this connection makes sense when noting that Charming Kitten's activity last year to exploit the ProxyShell vulnerability – an RCE flaw in Microsoft Exchange servers that suffered a barrage of attacks – "took place in about the same time frame as Memento," Frank observed.

"Iranian threat actors were also reported to be turning to ransomware during that period, which strengthens the hypothesis that Memento is operated by an Iranian threat actor," he wrote.

Organizations on Alert

Charming Kitten's continuous evolution of its capabilities has been well-documented, so its new tools and potential to branch out in terms of the type of attacks it can deliver should come as little surprise.

Indeed, threat groups in general are just like any legitimate businesses in that they must bob and weave constantly to meet business objectives, especially when old tactics don't serve them anymore or authorities are on to them, noted one security professional.

"Cybercriminals, like any business, work to evolve their software to improve, evolve and scale to bring about the best results needed to be successful," observed James McQuiggan, security awareness advocate at KnowBe4, in an email to Threatpost.

In the same way, organizations need to constantly be on their toes and create "a strong security culture" so they aren't caught unawares by novel tactics used by APTs like Charming Kitten and other highly organized threat groups, he said.

Source: https://threatpost.com/charming-kitten-powershell-backdoor/178158/

4. ESET antivirus bug let attackers gain Windows SYSTEM privileges

Slovak internet security firm ESET released security fixes to address a high severity local privilege escalation vulnerability affecting multiple products on systems running Windows 10 and later or Windows Server 2016 and above.

The flaw (CVE-2021-37852) was reported by Michael DePlante of Trend Micro's Zero Day Initiative, and it enables attackers to escalate privileges to NT AUTHORITY\SYSTEM account rights (the highest level of privileges on a Windows system) using the Windows Antimalware Scan Interface (AMSI).

AMSI was first introduced with Windows 10 Technical Preview in 2015, and it allows apps and services to request memory buffer scans from any major antivirus product installed on the system.

According to ESET, this can only be achieved after attackers gain SeImpersonatePrivilege rights, normally assigned to users in the local Administrators group and the device's local Service account to impersonate a client after authentication which should "limit the impact of this vulnerability."

However, ZDI's advisory says attackers are only required to "obtain the ability to execute low-privileged code on the target system," which matches ESET's CVSS severity rating also showing that the bug can be exploited by threat actors with low privileges.

While ESET said it only found out about this bug on November 18, a disclosure timeline available in ZDI's advisory reveals that the vulnerability was reported four months earlier, on June 18, 2021.

Affected ESET products

The list of products impacted by this vulnerability is quite long, and it includes:

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, and ESET Smart Security Premium from version 10.0.337.1 to 15.0.18.0
- ESET Endpoint Antivirus for Windows and ESET Endpoint Security for Windows from version 6.6.2046.0 to 9.0.2032.4
- ESET Server Security for Microsoft Windows Server 8.0.12003.0 and 8.0.12003.1, ESET File Security for Microsoft Windows Server from version 7.0.12014.0 to 7.3.12006.0
- ESET Server Security for Microsoft Azure from version 7.0.12016.1002 to 7.2.12004.1000
- ESET Security for Microsoft SharePoint Server from version 7.0.15008.0 to 8.0.15004.0
- ESET Mail Security for IBM Domino from version 7.0.14008.0 to 8.0.14004.0
- ESET Mail Security for Microsoft Exchange Server from version 7.0.10019 to 8.0.10016.0

Users of ESET Server Security for Microsoft Azure are also advised to immediately update ESET File Security for Microsoft Azure to the latest available version of ESET Server Security for Microsoft Windows Server to address the flaw.

The antivirus maker released multiple security updates between December 8 and January 31 to address this vulnerability, when it patched the last vulnerable product exposed to attacks.

Luckily, ESET found no evidence of exploits designed to target products affected by this security bug in the wild.

"The attack surface can also be eliminated by disabling the Enable advanced scanning via AMSI option in ESET products' Advanced setup," ESET added.

"However, ESET strongly recommends performing an upgrade to a fixed product version and only applying this workaround when the upgrade is not possible for an important reason."

Source: https://www.bleepingcomputer.com/news/microsoft/eset-antivirus-bug-let-attackers-gain-windows-system-privileges/

5. MFA adoption pushes phishing actors to reverse-proxy solutions

The rising adoption of multi-factor authentication (MFA) for online accounts pushes phishing actors to use more sophisticated solutions to continue their malicious operations, most notably reverse-proxy tools.

The COVID-19 pandemic has changed the way people work forever, proving that it's possible and sometimes even preferable to work from home.

This has increased security risks for companies, many of which can be mitigated by using MFA to protect their employees' accounts.

Even Google, a key internet services provider, has recently decided to enforce two-factor authentication (2FA) on all Google accounts through a staged auto-enrollment process.

With MFA, a user must provide a second authentication factor apart from their account's password to access it. This factor can be a one-time code sent via SMS or email, a token, or a unique cryptographic key.

This additional step creates a practical problem for phishing actors, as stealing the account credentials is no longer enough for them to assume control of them.

Natural evolution

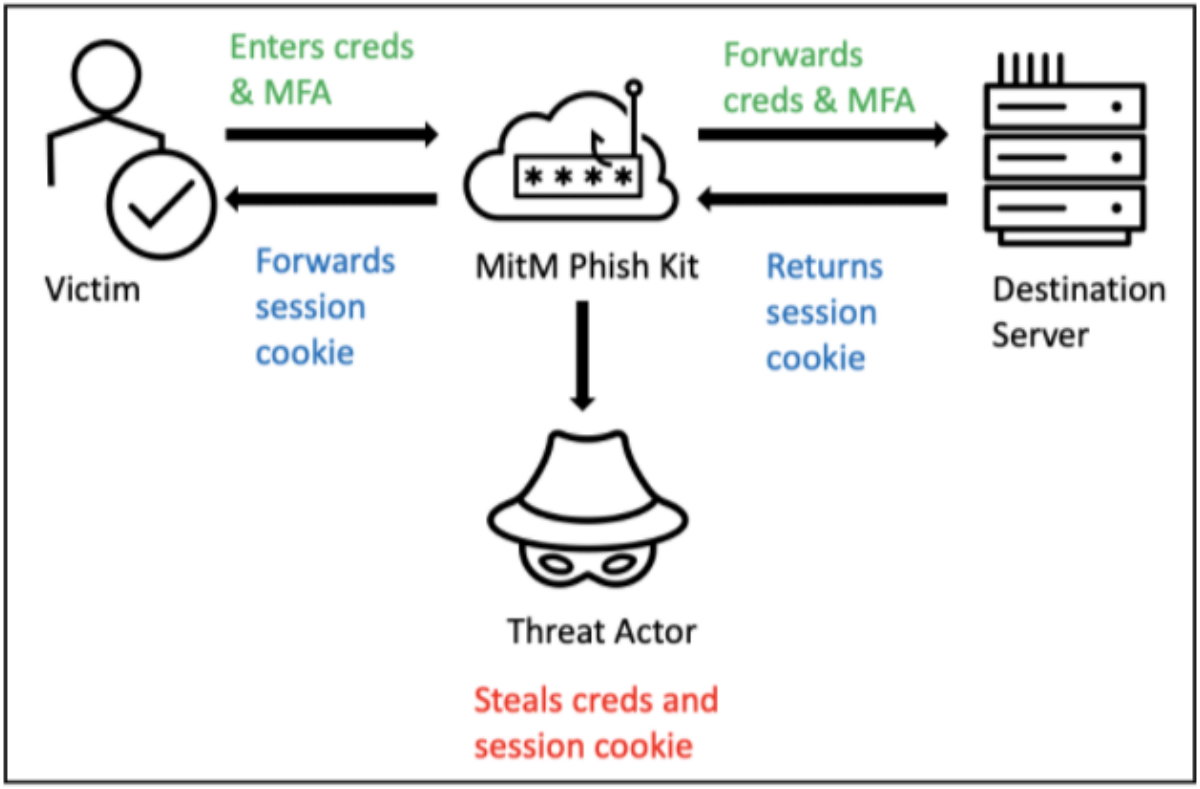
The increasing use of MFA has pushed phishing actors to use transparent reverse proxy solutions, and to cover this rising demand, reverse proxy phish kits are being made available.

A reverse proxy is a server that sits between the Internet user and web servers behind a firewall. The reverse proxy then forwards visitors' requests to the appropriate servers and sends back the resulting response. This allows a webserver to serve requests without making itself directly available on the Internet.

As detailed in a report published today by Proofpoint, new phishing kits have emerged that offer templates to create convincing login web pages that mimic popular sites.

These newer kits are more advanced because they now integrate an MFA snatching system, which enables threat actors to steal login credentials and MFA codes that would normally protect the account.

As depicted below, when a victim logs into the phishing page, the kit sends the MFA to the genuine online service, intercepts the session cookie, and optionally forwards it to the victim.



How reverse proxy phishing attacks work
Source: Proofpoint

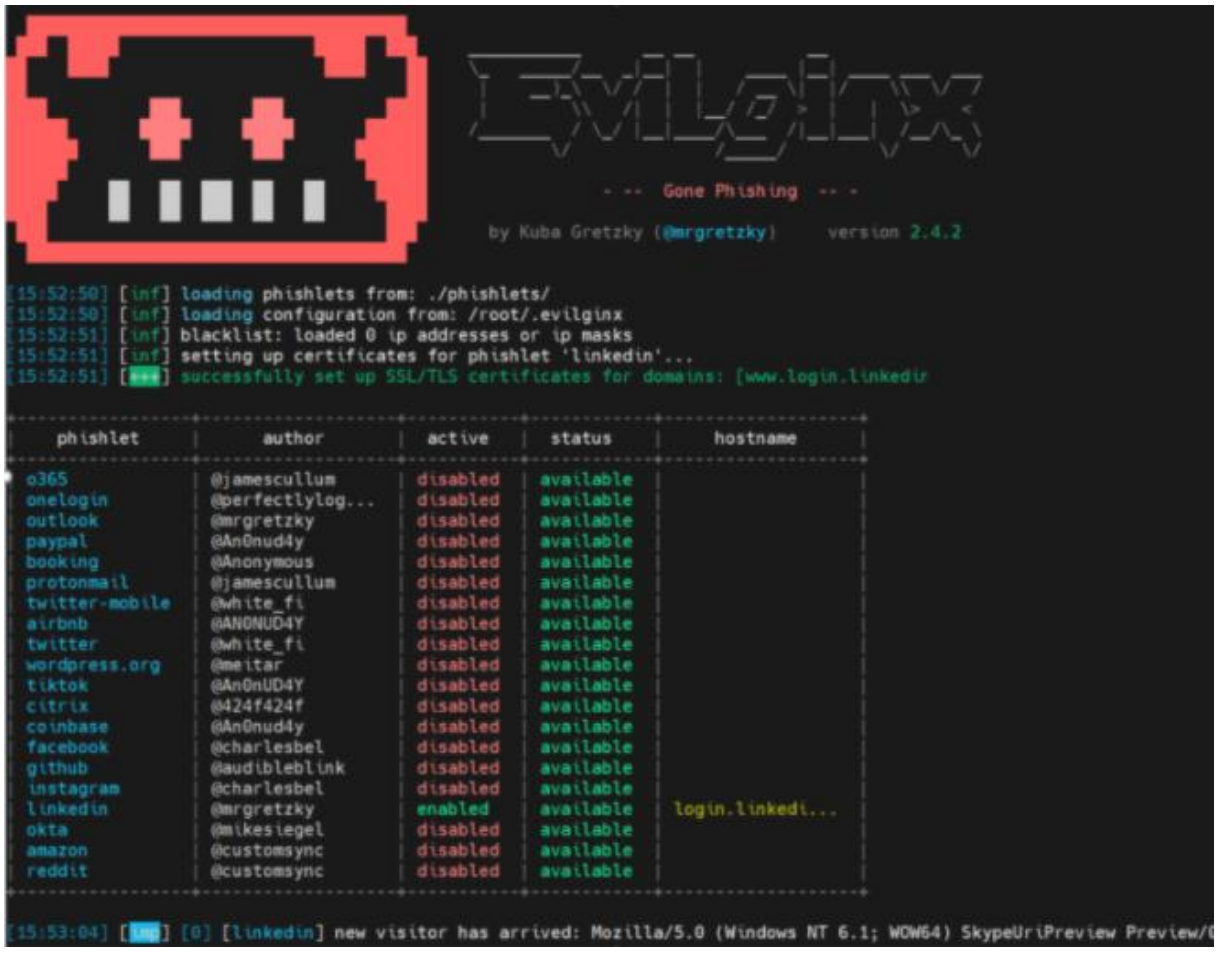
This allows the victim to log in to the actual site and raise no suspicions. Meanwhile, the threat actors have stolen both the credentials and the cookie needed to access the account.

Proofpoint has seen three kinds of phishing kits that employ reverse proxying systems, one using Modlishka, another using Muraena/Necrobrowser, and one relying on Evilginx2.

Modlishka is the least sophisticated of the bunch, created as a demonstration in 2018, but it's still capable of harvesting a victim's session even when push notification systems are employed.

Necrobrowser was released in 2019, offering additional capabilities such as auto-login, password changing, disabling Google Workspace notifications, dumping emails, changing SSH session keys, downloading repositories from GitHub, etc.

Evilginx2 relies on a proprietary system of configurable "phishlets" which enable threat actors to target any site they want. The kit features several pre-installed "phishlets" too, so one can get started right away.



Some of the phislets offered by Evilginx2 out of the box
Source: Proofpoint

A blind spot in security

Although the existence and implications of these tools have been well documented, the problem remains largely unaddressed, and as more phishing actors turn to using them, making MFA less secure.

One way to tackle the problem is to identify the man-in-the-middle pages used in these attacks. However, as the findings of a recent study have shown, only about half of those are blocklisted at any given time.

The constant refresh of domains and IP addresses used for reverse proxy attacks reduces the effectiveness of blocklists, as most of these last between 24 and 72 hours.

As such, the only method that may fight the problem is to add client-side TLS fingerprinting, which could help identify and filter MITM requests.

Source: https://www.bleepingcomputer.com/news/security/mfa-adoption-pushes-phishing-actors-to-reverse-proxy-solutions/

6. State hackers' new malware helped them stay undetected for 250 days

A state-backed Chinese APT actor tracked as 'Antlion' has been using a new custom backdoor called 'xPack' against financial organizations and manufacturing companies.

The malware has been used in a campaign against targets in Taiwan that researchers believe spanned for more than 18 months, between 2020 and 2021, allowing the adversaries to run stealthy cyber-espionage operations.

According to a report from Symantec, a Broadcom company, shared with BleepingComputer, xPack enabled attackers to run WMI commands remotely, to leverage EternalBlue exploits, and mounted shares over SMB to deliver data to the command and control (C2) server.

In the network for 250 days

Details from one attack show that the threat actor spent 175 days on the compromised network. However, Symantec researchers analyzing two other attacks determined that the adversary went undetected on the network for as long as 250 days.

Using custom malware unknown to threat analysts played a key role in achieving this level of stealthiness.

xPack is a .NET loader that fetches and executes AES-encrypted payloads, while it's also capable to execute system commands and stage data for exfiltration.

Symantec also spotted the following custom tools that accompanied xPack in this camapaign:

- **EHAGBPSL** – Custom C++ loader
- **JpgRun** – Custom C++ loader
- **CheckID** – Custom C++ loader based on a similar tool used by the BlackHole RAT
- **NetSessionEnum** – Custom SMB session enumeration tool
- **ENCODE MMC** – Custom bind/reverse file transfer tool
- Kerberos golden ticket tool based on the Mimikatz credentials stealer

Antlion also used various off-the-shelf and living-off-the-land (LoL) tools in combination with the above to achieve full operational capability without raising security flags.

Tools such as PowerShell, WMIC, ProcDump, LSASS, and PsExec were common in this campaign, leaving crumbs of evidence that easily blend with ordinary operating system functions.

Finally, the actors were also observed leveraging CVE-2019-1458 for privilege escalation and remote scheduling that helped execute the backdoor.

This vulnerability was recently included on CISA's list of actively exploited flaws, so it's still an attractive avenue for multiple adversaries.

"There is also evidence that the attackers likely automated the data collection process via batch scripts, while there is also evidence of instances where data was likely staged for further exfiltration, though it was not actually observed being exfiltrated from the network," explains Symantec

"In these instances, it appears the attackers were interested in collecting information from software pertaining to business contacts, investments, and smart card readers."

In the attacks dissected by Symantec's analysts, xPack was initially used to collect basic system information and running processes, and then for dumping credentials.

Afterwards, the actors returned periodically and launched xPack again to steal account credentials from several machines in the compromised organizations.

Antlion still active and dangerous

Antlion is believed to be involved in cyber-espionage activities since at least 2011, so this is an actor that has remained a threat to organizations for over a decade now.

Its interest in targeting Taiwanese firms has political extensions and is in line with the operational strategy of most Chinese state-sponsored groups.

As detailed in Symantec's report, the particular campaign focused on dumping credentials from the compromised systems and then using them to move laterally.

It's possible that Antlion shared these credentials with other Chinese hacker groups that had a different operational focus, as it is common for actors working for the same state to collaborate.

Source: https://www.bleepingcomputer.com/news/security/state-hackers-new-malware-helped-them-stay-undetected-for-250-days/

7. China Suspected of News Corp Cyberespionage Attack

Attackers infiltrated the media giant's network using BEC, while Microsoft moved to stop such attacks by blocking VBA macros in 5 Windows apps. Included: more ways to help stop BEC.

The Chinese hackers responsible for an attack on media giant News Corp last month likely were seeking intelligence to serve China's interests in a cyberespionage incident that shows the persistent vulnerability of corporate networks to email-based attacks, security professionals said.

Reports on Monday revealed that a Jan. 20 incident at Rupert Murdoch's media giant involved an attack on journalists' email accounts that gave the intruders access to sensitive data. The breach – limited to several individuals working for outlets including News UK, the Wall Street Journal and the New York Post – has raised concerns over the safety of confidential sources working with journalists affected by the incident.

In an email to staff, News Corp cited a "foreign government" as responsible for the "persistent nation-state attack" and confirmed that "some data" was stolen, according to published reports. The media giant enlisted the help of cybersecurity firm Mandiant to investigate the incident, which the firm said is likely the work of a China-sponsored actor.

"Mandiant assesses that those behind this activity have a China nexus, and we believe they are likely involved in espionage activities to collect intelligence to benefit China's interests," said David Wong, vice president of consulting at Mandiant, in an emailed statement to Threatpost.

Targeting Journalists for Cyberespionage

Indeed, while China typically targets "military and intellectual property" in its state-sponsored attacks, journalists also are "fairly high on their radar for espionage" due to their work with sources – confidential and otherwise, as noted by one cybersecurity professional.

"Journalists can have access to sources and intelligence about adversaries and other opponents of the Chinese regime, both foreign and domestic, or can be researching stories that could generate negative publicity for the Chinese government," Mike McLellan, director of intelligence for cyber threat intelligence firm Secureworks Counter Threat Unit, wrote in an email to Threatpost on Monday.

Paul Farrington, chief product officer for security firm Glasswall, agreed that it's "common for politically motivated cybercriminals to mine reporters' materials for intelligence," given their frequent conversations with confidential sources that have access to information about current and future geopolitical events.

Moreover, China has previously shown an interest in attacking journalists, making this latest attack "entirely consistent with past Chinese state-sponsored behavior," concurred Dave Merkel, CEO of cybersecurity firm Expel.

He cited a previous attack on the New York Times by China in 2013 as a precedent for the nation's targeting of journalists. Moreover, the threat actors' use of business email compromise (BEC) to pull off the attack "makes sense" and also is consistent with nation-state actors, Merkel observed.

"When it comes to cyberattacks, nation state actors will only be as advanced as they have to – why burn expensive zero days if you don't need to?" he said.

Preventing BEC Attacks

In fact, Merkel said the No. 1 source of attacks against Expel customers is BEC. "There's no reason to think Chinese state-sponsored groups wouldn't use the same tactics against their targets if those tactics work – and news organizations are definitely targets," he said.

Indeed, BEC is a major threat that typically involves human error. The way it works is that an employee at a company receives an email with a malicious link or document and takes an action that can install malware on their computers. This can result in consequences from local data theft to giving threat actors access to the corporate network to advanced attack vectors such as ransomware.

Microsoft unveiled a timely yet unrelated step this week that could help mitigate the impact of, or even prevent, future BEC attacks: Namely, the company will soon begin blocking, by default, VBA macros obtained from the internet in five Office apps, as the company revealed in a blog post Monday.

"For macros in files obtained from the internet, users will no longer be able to enable content with a click of a button," Microsoft Principal Program Manager Kellie Eickmeyer wrote. "A message bar will appear for users notifying them with a button to learn more."

This default setting "is more secure and is expected to keep more users safe including home users and information workers in managed organizations," she added. Indeed, sending documents loaded with macros that immediately install malware on people's computers with one click is a popular tactic of email-based attacks.

The new default setting will apply to Microsoft Office on devices running Windows for Access, Excel, PowerPoint, Visio and Word. Microsoft will roll out the change first in a preview version of Office 2023, starting with its Current Channel update channel in early April 2022.

Later, the change will be available in the other update channels, such as Current Channel, Monthly Enterprise Channel, and Semi-Annual Enterprise Channel. In the future Microsoft also will change the Office default setting for VBA macros in Office LTSC, Office 2021, Office 2019, Office 2016 and Office 2013, Eickmeyer added.

This move may make it more difficult to slip malware past corporate employees using BEC tactics. However, as one security professional noted, companies still must remain vigilant and take an "all hands on deck" approach to both threat mitigation and response, given the evolving nature and increased occurrence of cyber-attacks that organizations face.

"As the threat environment continues to change, proper and continuous diligence is required to ensure all cyber defensive tools and techniques are employed to protect your most precious data assets," observed Tom Garrubba, vice president at risk-management firm Shared Assessments**,** in an email to Threatpost. "Continuous intelligence, monitoring, and dialogue with critical partners and suppliers should be ongoing to ensure 'all is ready' in the event recovery is needed, and that additional support is available in the event something were to occur."

Source: https://threatpost.com/china-suspected-news-corp-cyberespionage/178277/

8. US seizes $3.6 billion stolen in 2016 Bitfinex cryptoexchange hack

The US Department of Justice announced that law enforcement seized billions worth of cryptocurrency linked to the 2016 Bitfinex cryptocurrency exchange hack.

A Manhattan couple, Ilya Lichtenstein, 34, and his wife, Heather Morgan, 31, were arrested today for allegedly being involved in a conspiracy to launder the stolen cryptocurrency.

In 2016, the 119,756 bitcoins stolen during the attack were worth almost $78 million and are now valued at roughly $4.5 billion.

DOJ officials said the funds were recovered after IRS-Criminal Investigation (IRS-CI) special agents executed "court-authorized search warrants of online accounts controlled by Lichtenstein and Morgan" to seize files with the private keys required to access the wallets containing the stolen Bitfinex bitcoins.

"Those files contained the private keys required to access the digital wallet that directly received the funds stolen from Bitfinex, and allowed special agents to lawfully seize and recover more than 94,000 bitcoin that had been stolen from Bitfinex. The recovered bitcoin was valued at over $3.6 billion at the time of seizure," DOJ said.

"Today's arrests, and the department's largest financial seizure ever, show that cryptocurrency is not a safe haven for criminals," added Deputy Attorney General Lisa O. Monaco.

Lichtenstein and Morgan were charged today with conspiracy to commit money laundering, which comes with a maximum sentence of 20 years in prison, and conspiracy to defraud the USA, which also carries a maximum sentence of five years.

Largest cryptocurrency seizure ever

According to Chief Jim Lee of IRS-Criminal Investigation (IRS-CI), this was the largest cryptocurrency seizure ever made by DOJ.

"IRS-CI Cyber Crimes Unit special agents have once again unraveled a sophisticated laundering technique, enabling them to trace, access and seize the stolen funds, which has amounted to the largest cryptocurrency seizure to date, valued at more than $3.6 billion," Lee said.

The defendants allegedly attempted to launder the stolen cryptocurrency by making deposits on the AlphaBay dark web marketplace, as well as buying gift cards from Uber, Hotels.com, PlayStation, and Walmart.

Court documents show that the couple allegedly used sophisticated laundering techniques, including:

- using fictitious identities to set up online accounts;
- utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time;
- depositing the stolen funds into accounts at a variety of virtual currency exchanges and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow;
- converting bitcoin to other forms of virtual currency, including anonymity-enhanced virtual currency (AEC), in a practice known as "chain hopping";
- and using U.S.-based business accounts to legitimize their banking activity.

More info on how the stolen Bitfinex funds were traced and were moved to accounts linked to the two defendants can be found in this statement of facts released today by DOJ.

"Bitfinex will work with the DOJ and follow appropriate legal processes to establish our rights to a return of the stolen bitcoin," the Hong Kong cryptocurrency exchange said in a statement today.

"Bitfinex intends to provide further updates on its efforts to obtain a return of the stolen bitcoin as and when those updates are available."

Source: https://www.bleepingcomputer.com/news/security/us-seizes-36-billion-stolen-in-2016-bitfinex-cryptoexchange-hack/

9. Fake Windows 11 upgrade installers infect you with RedLine malware

Threat actors have started distributing fake Windows 11 upgrade installers to users of Windows 10, tricking them into downloading and executing RedLine stealer malware.

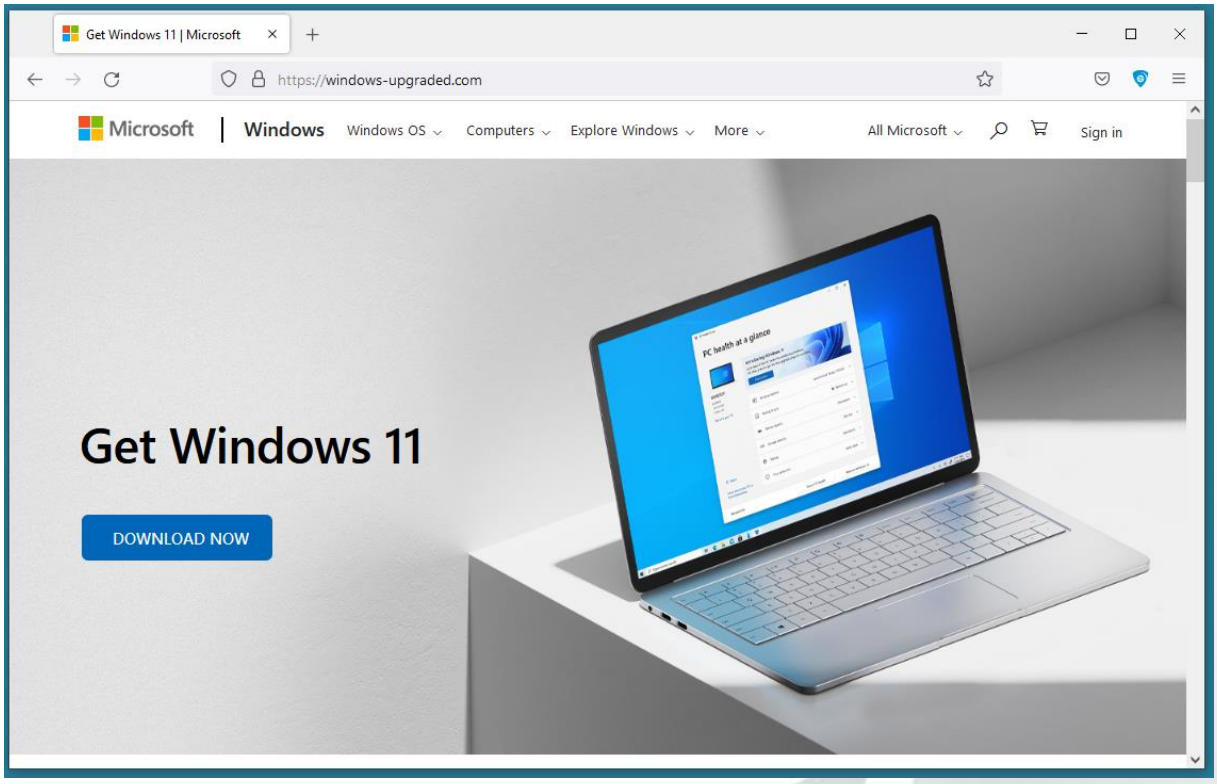
The timing of the attacks coincides with the moment that Microsoft announced Windows 11's broad deployment phase, so the attackers were well-prepared for this move and waited for the right moment to maximize their operation's success.

RedLine stealer is currently the most widely deployed password, browser cookies, credit card, and cryptocurrency wallet info grabber, so its infections can have dire consequences for the victims.

The campaign

According to researchers at HP, who have spotted this campaign, the actors used the seemingly legitimate "windows-upgraded.com" domain for the malware distribution part of their campaign.

The site appears like a genuine Microsoft site and, if the visitor clicked on the 'Download Now' button, they received a 1.5 MB ZIP archive named "Windows11InstallationAssistant.zip," fetched directly from a Discord CDN.



Fake website used for malware distribution (HP)

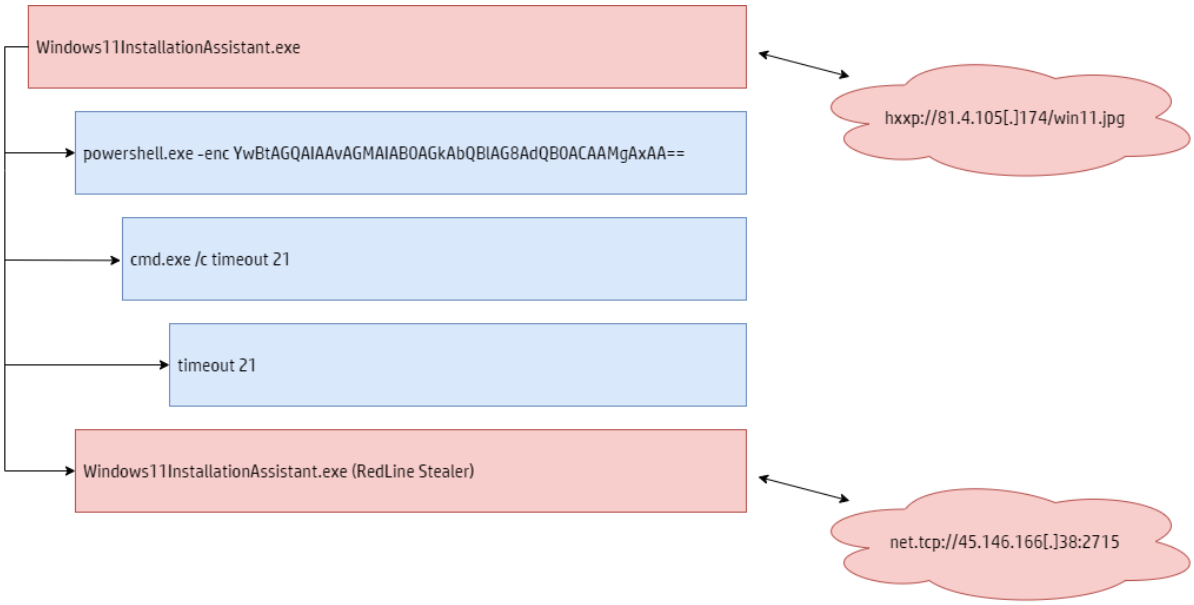
Decompressing the file results in a folder of 753MB of size, showcasing an impressive compression ratio of 99.8%, achieved thanks to the presence of padding in the executable.

When the victim launches the executable in the folder, a PowerShell process with an encoded argument starts.

Next, a cmd.exe process is launched with a timeout of 21 seconds, and after that expires, a .jpg file is fetched from a remote web server.

This file contains a DLL with contents arranged in reverse form, possibly to evade detection and analysis.

Finally, the initial process loads the DLL and replaces the current thread context with it. That DLL is a RedLine stealer payload that connects to the command-and-control server via TCP to get instructions on what malicious tasks it has to run next on the newly compromised system.



RedLine execution and loading chain (HP)

Outlook

Although the distribution site is down now, nothing stops the actors from setting up a new domain and restarting their campaign. In fact, this is very likely already happening in the wild.

Windows 11 is a major upgrade that many Windows 10 users cannot get from the official distribution channels due to hardware incompatibilities, something that malware operators see as an excellent opportunity for finding new victims.

As BleepingComputer reported in January, threat actors are also leveraging Windows' legitimate update clients to execute malicious code on compromised Windows systems, so the tactics reported by HP are hardly surprising at this point.

Remember, these dangerous sites are promoted via forum and social media posts or instant messages, so don't trust anything but the official Windows upgrade system alerts.

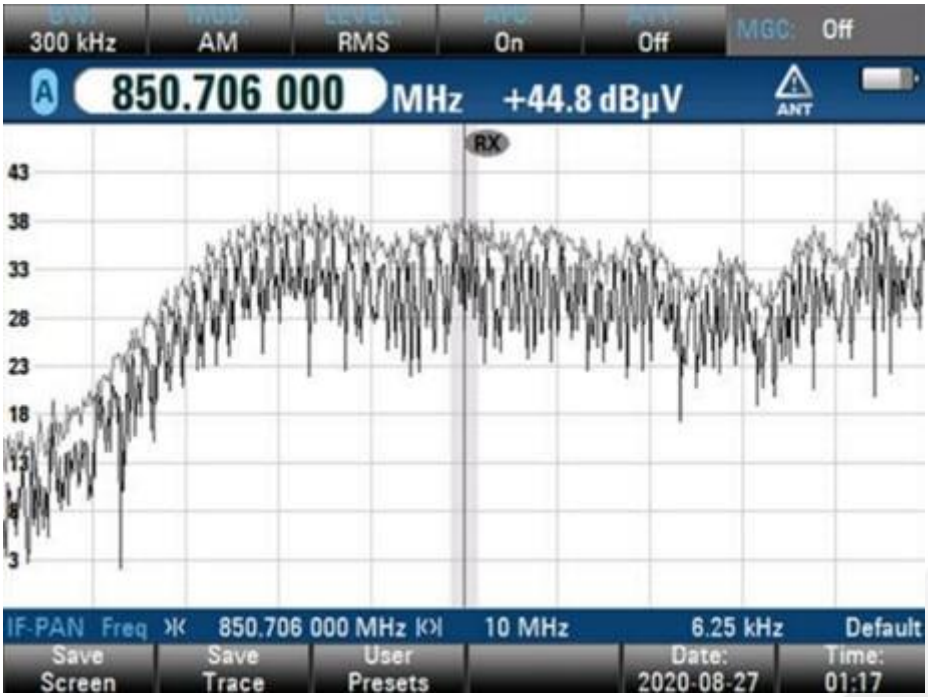
Source: https://www.bleepingcomputer.com/news/security/fake-windows-11-upgrade-installers-infect-you-with-redline-malware/

10. Dad takes down town's internet by mistake to get his kids offline

A French dad faces jail time and a hefty fine after using a signal jammer to prevent his kids from going online and taking the rest of a nearby town down with them.

Starting at midnight and until 3 AM every day of the week, the French town of Messanges found that their cellular and Internet service were no longer working.

After a mobile carrier reported the issue to the Agence nationale des fréquences (ANFR), a public agency responsible for managing the radioelectric spectrum in France, it was determined that a signal jammer was being used to block radio frequencies in the town.



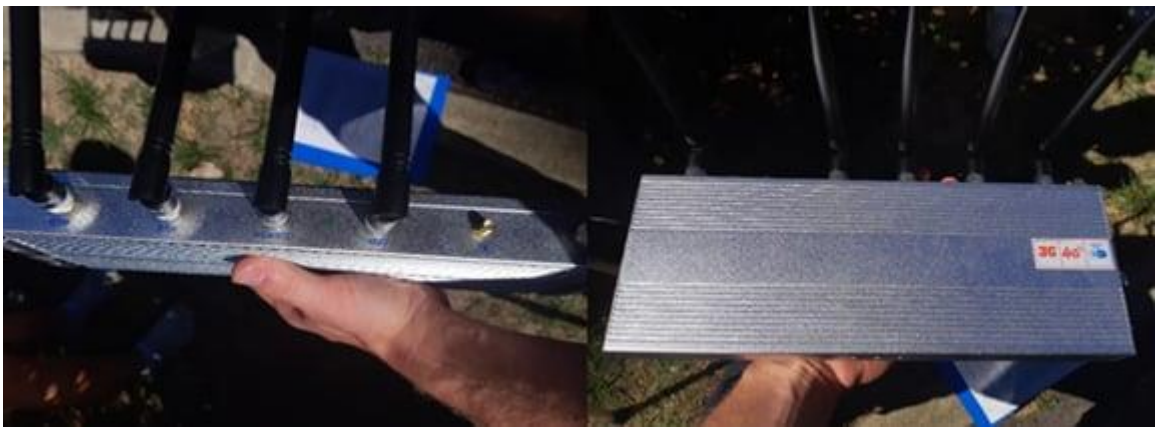
Graph displaying the signature of a signal jammer
Source: ANFR

A signal jammer is a device that transmits radio waves on the same frequency as mobile devices to prevent them from connecting to cell towers and receiving legitimate signals.

A report by the ANFR explains that a technician traced the jamming signal to a house in a neighboring town, where a homeowner admitted to purchasing a jammer online and using it to force his teenage kids offline.

"The explanation was disconcertingly simple: the jammer had been installed by the father of the family to prevent his teenagers from accessing the internet with their smartphone instead of falling asleep! His children had indeed become addicted to social networks and other applications, in particular since the confinement imposed due to the epidemic of Covid-19," ANFR explained in their report.

"After consulting forums on the internet, the father decided that a jammer was the best solution to put an end to these excesses!"



The jammer seized by ANFR
Source: ANFR

While it was not the father's intent to take down an entire town's Internet, using a jamming device in France is illegal and carries a penalty of up to a €30,000 fine and 6 months in jail.

Similarly, the use of jammers is illegal in the USA and could lead to imprisonment and significant monetary fines.

"The use or marketing of a jammer in the United States may subject you to substantial monetary penalties, seizure of the unlawful equipment, and criminal sanctions including imprisonment." explains an FCC enforcement alert about jamming.

The ANFR reported the use of the jammer to the Public Prosecutor's office, who has seized the device and is investigating the offense.

Source: https://www.bleepingcomputer.com/news/technology/dad-takes-down-towns-internet-by-mistake-to-get-his-kids-offline/

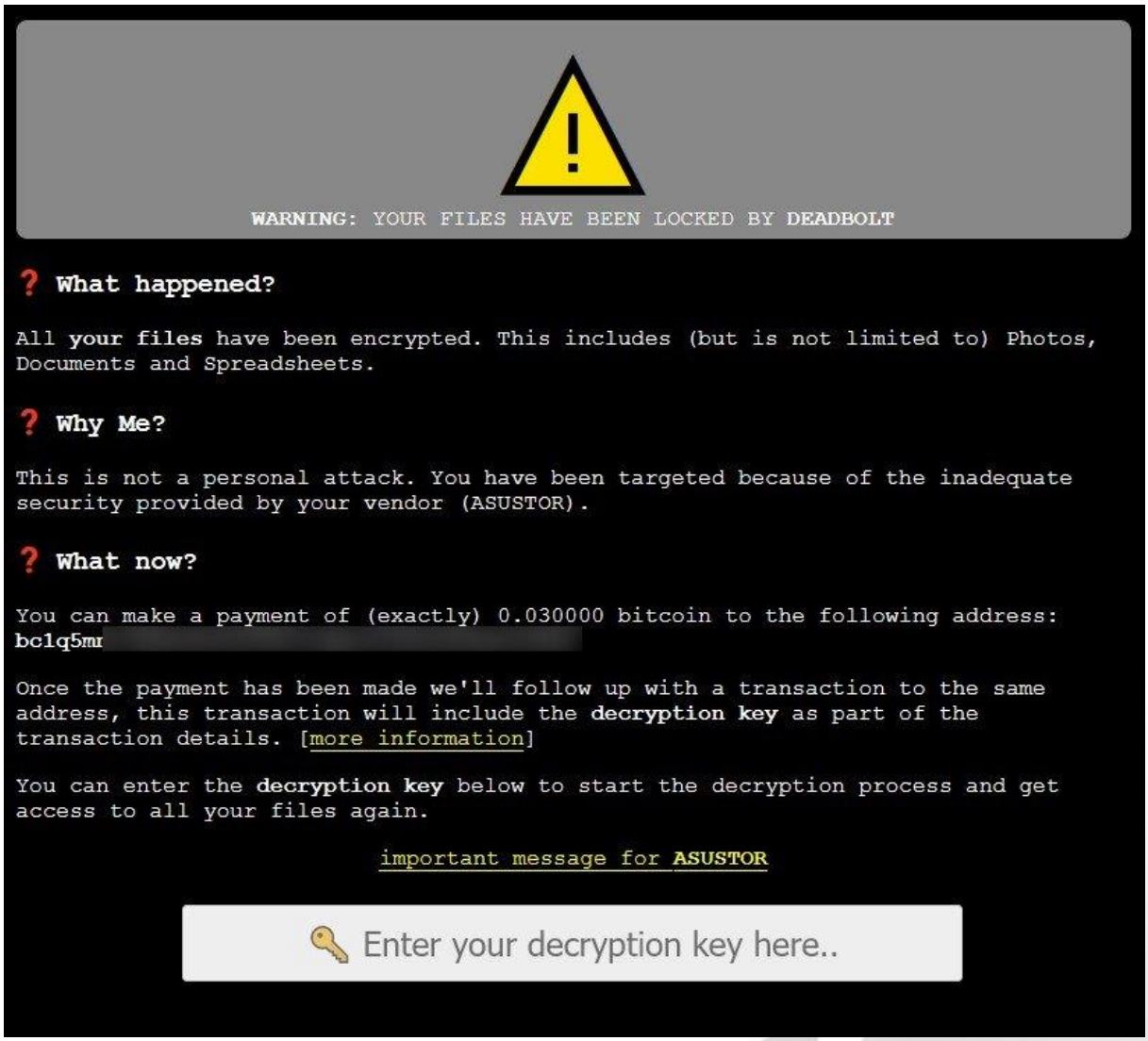
11. DeadBolt ransomware now targets ASUSTOR devices, asks 50 BTC for master key

The The DeadBolt ransomware is now targeting ASUSTOR NAS devices by encrypting files and demanding a $1,150 ransom in bitcoins.

This wave of attacks was first reported on Reddit and the BleepingComputer forums, and soon after, on the ASUSTOR forums.

Similar to the DeadBolt ransomware attacks that targeted QNAP NAS devices last month, the threat actors claim to be using a zero-day vulnerability to encrypt ASUSTOR NAS devices.

When encrypting files on an ASUSTOR device, the ransomware will rename the files to include the **.deadbolt** file extension. The ASUSTOR login screen will also be replaced with a ransom note demanding 0.03 bitcoins, worth approximately $1,150, as shown below.



DeadBolt ransom note on ASUSTOR NAS device
Source: BleepingComputer.com

While ASUSTOR has not explained how the NAS devices are being encrypted, some ASUSTOR owners believe that it is a vulnerability in the PLEX media server or EZ Connect that allows access to their devices.

ASUSTOR states that they are investigating the attacks and have provided the following statement:

In response to Deadbolt ransomware attacks affecting ASUSTOR devices, the myasustor.com DDNS service will be disabled as the issue is investigated. ASUSTOR will release more information with new developments as we investigate and review the causes to ensure this does not happen again. We remain committed to helping affected customers in every way possible. For your protection, we recommend the following measures:

Change default ports, including the default NAS web access ports of 8000 and 8001, as well as remote web access ports of 80 and 443.

- Disable EZ Connect.
- Close Plex Ports and disable Plex.
- Make an immediate backup.
- Turn off Terminal/SSH and SFTP services.

Most importantly, do not expose your ASUSTOR device to the Internet to avoid being encrypted by DeadBolt.

If DeadBolt has already infected your device, unplug the Ethernet cable and force-shut down your NAS device by holding the power button for three seconds.

Do not attempt to reboot the NAS, as this will erase all files. Instead, use this contact form to request instructions from ASUSTOR technicians on how to recover your files.

It is unclear if all ASUSTOR devices are vulnerable to DeadBolt attacks, but reports indicate that the AS6602T, AS-6210T-4K, AS5304T, AS6102T, and AS5304T models are unaffected.

Unfortunately, there is no way to recover files encrypted by the DeadBolt ransomware for free, and many affected QNAP users were forced to pay the ransom to recover files.

Recovery firmware to be released today

ASUSTOR is planning to release a recovery firmware today so that users can once again use their NAS devices. However, this firmware update will not help recover any encrypted files.

"We estimate to release a recovery firmware from our support engineers today for users whose NAS is hacked so they can use their NAS again. However, encrypted files can not be recovered unless users have backups," ASUSTOR wrote to their Facebook page.

Unfortunately, this recovery process will likely remove the ransom note pages and malware executable required to decrypt files if a ransom is paid, which historically caused a lot of issues for QNAP owners.

It is strongly suggested that users backup the **index.cgi** and **ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT.html** files before running the recovery software.

These files contain the information necessary to pay the ransom and receive a decryption key, which owners can then use with Emsisoft's decryptor for DeadBolt.

If a ransom is paid, the threat actors will create a bitcoin transaction to the same bitcoin address a ransom was paid that contains the decryption key for the victim. The decryption key is located under the OP_RETURN output, as shown below.

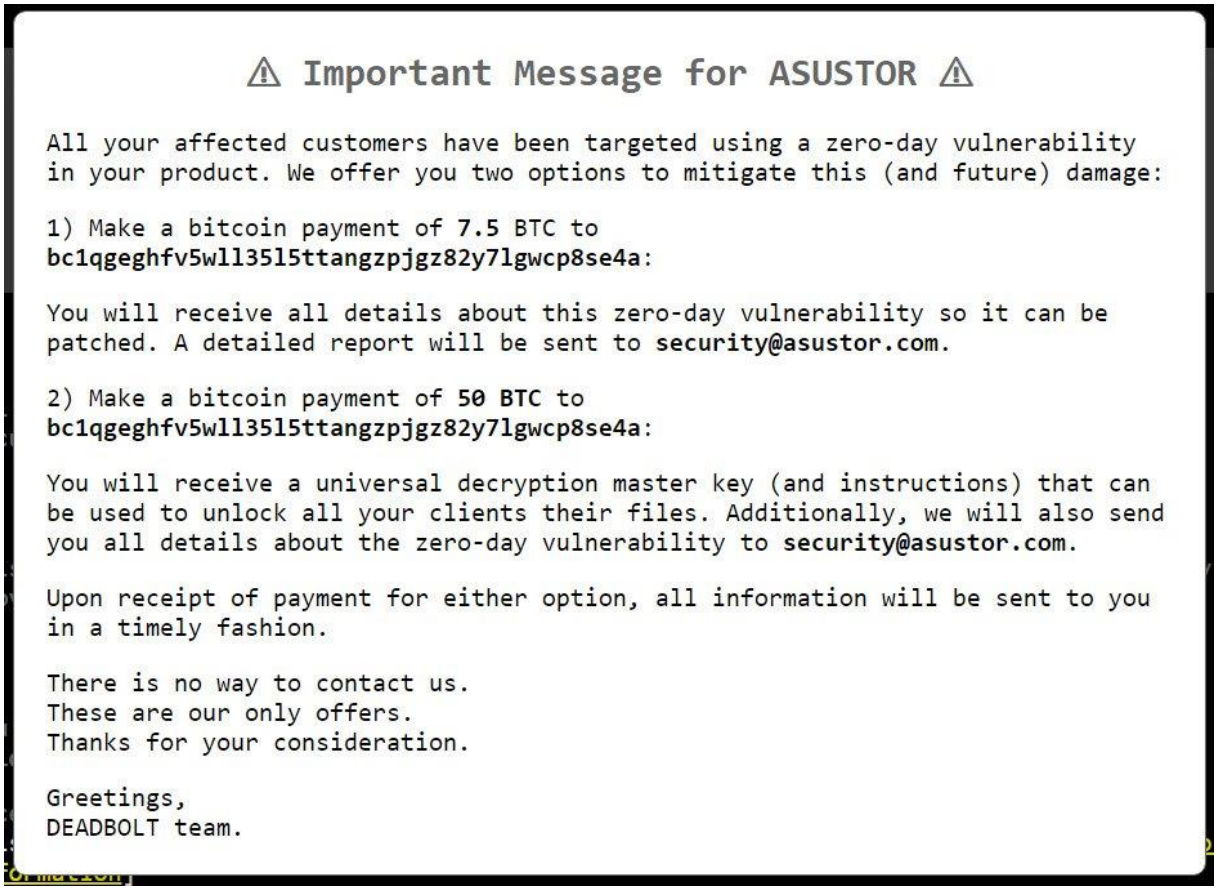
Bitcoin transaction's OP_RETURN output containing decryption key
Source: BleepingComputer

For those who need help with the decryption process or want to see common issues that affected QNAP devices last month, you can review our DeadBolt ransomware support topic.

Demanding 50 bitcoin for a master key

Similar to the attacks on QNAP devices, DeadBolt is attempting to sell information to ASUSTOR about the alleged zero-day vulnerability used to breach NAS devices and the master decryption for all victims.

The DeadBolt ransom note includes a link titled "important message for ASUSTOR," that when clicked, will display a message from the DeadBolt gang specifically for ASUSTOR.



DeadBolt message for ASUSTOR
Source: BleepingComputer

On this screen, the DeadBolt threat actors are selling the details of the alleged zero-day vulnerability if ASUSTOR pays them 7.5 Bitcoins, worth $290,000.

The DeadBolt gang is also trying to sell ASUSTOR the master decryption key for all victims and the zero-day details for 50 bitcoins, worth $1.9 million.

"Make a bitcoin payment of 50 BTC to bc1qgeghfv5wll35l5ttangzpjgz82y7lgwcp8se4a," the threat actors wrote in a message to QNAP.

"You will receive a universal decryption master key (and instructions) that can be used to unlock all your clients their files. Additionally, we will also send you all details about the zero-day vulnerability to security@asustor.com."

The ransomware operation states that there is no way to contact them other than making the bitcoin payment. However, once payment is made, they say they will send the information to the security@asustor.com email address.

It is doubtful that ASUSTOR will pay the extortion demand, so if the DeadBolt Ransomware encrypted your NAS device, the only way to recover files is to restore from backups or pay the ransom.

Based on last month's analysis of the ransomware by BleepingComputer, DeadBolt is a Linux malware that uses a template for the ransom note that can be substituted for any vendor, as shown below:

```
This is not a personal attack. You have been targeted because of the
inadequate security provided by your vendor ({VENDOR_NAME}).
```

Therefore, we will likely see attacks against other NAS manufacturers in the future.

Source: https://www.bleepingcomputer.com/news/security/deadbolt-ransomware-now-targets-asustor-devices-asks-50-btc-for-master-key/

12. Samsung Shattered Encryption on 100M Phones

One One cryptography expert said that 'serious flaws' in the way Samsung phones encrypt sensitive material, as revealed by academics, are 'embarrassingly bad.'

Samsung shipped an estimated 100 million smartphones with botched encryption, including models ranging from the 2017 Galaxy S8 on up to last year's Galaxy S21.

Researchers at Tel Aviv University found what they called "severe" cryptographic design flaws that could have let attackers siphon the devices' hardware-based cryptographic keys: keys that unlock the treasure trove of security-critical data that's found in smartphones.

What's more, cyber attackers could even exploit Samsung's cryptographic missteps – since addressed in multiple CVEs – to downgrade a device's security protocols. That would set up a phone to be vulnerable to future attacks: a practice known as IV (initialization vector) reuse attacks. IV reuse attacks screw with the encryption randomization that ensures that even if multiple messages with identical plaintext are encrypted, the generated corresponding ciphertexts will each be distinct.

Untrustworthy Implementation of TrustZone

In a paper (PDF) entitled "Trust Dies in Darkness: Shedding Light on Samsung's TrustZone Keymaster Design" – written by by Alon Shakevsky, Eyal Ronen and Avishai Wool – the academics explain that nowadays, smartphones control data that includes sensitive messages, images and files; cryptographic key management; FIDO2 web authentication; digital rights management (DRM) data; data for mobile payment services such as Samsung Pay; and enterprise identity management.

The authors are due to give a detailed presentation of the vulnerabilities at the upcoming USENIX Security, 2022 symposium in August.

The design flaws primarily affect devices that use ARM's TrustZone technology: the hardware support provided by ARM-based Android smartphones (which are the majority) for a Trusted Execution Environment (TEE) to implement security-sensitive functions.

TrustZone splits a phone into two portions, known as the Normal world (for running regular tasks, such as the Android OS) and the Secure world, which handles the security subsystem and where all sensitive resources reside. The Secure world is only accessible to trusted applications used for security-sensitive functions, including encryption.

Cryptography Experts Wince

Matthew Green, associate professor of computer science at the Johns Hopkins Information Security Institute, explained on Twitter that Samsung incorporated "serious flaws" in the way its phones encrypt key material in TrustZone, calling it "embarrassingly bad."

"They used a single key and allowed IV re-use," Green said.

"So they could have derived a different key-wrapping key for each key they protect," he continued. "But instead Samsung basically doesn't. Then they allow the app-layer code to pick encryption IVs." The design decision allows for "trivial decryption," he said.

Paul Ducklin, principal research scientist for Sophos, called out Samsung coders for committing "a cardinal cryptographic sin." Namely, "They used a proper encryption algorithm (in this case, AES-GCM) improperly," he explained to Threatpost via email on Thursday.

"Loosely speaking, AES-GCM needs a fresh burst of securely chosen random data for every new encryption operation – that's not just a 'nice-to-have' feature, it's an algorithmic requirement. In internet standards language, it's a MUST, not a SHOULD," Ducklin emphasized. "That fresh-every-time randomness (12 bytes' worth at least for the AES-GCM cipher mode) is known as a 'nonce,' short for Number Used Once – a jargon word that cryptographic programmers should treat as an *command*, not merely as a noun."

Unfortunately, Samsung's supposedly secure cryptographic code didn't enforce that requirement, Ducklin explained. "Indeed, it allowed an app running outside the secure encryption hardware component not only to influence the nonces used inside it, but even to choose those nonces exactly, deliberately and malevolently, repeating them as often as the app's creator wanted."

By exploiting this loophole, the researchers were able to pull off a feat that's "supposed to be impossible, or as close to impossible as possible," he continued. Namely, the team were able to "extract cryptographic secrets from *inside* the secure hardware."

So much for all the encryption security that the special hardware is supposed to enforce, Ducklin mused, as demonstrated by the researchers' multiple proof-of-concept security bypass attacks.

Ducklin's admonishment: "Simply put, when it comes to using proper encryption properly: Read The Full Manual!"

Flaws Enable Security Standards Bypass

The security flaws not only allow cybercriminals to steal cryptographic keys stored on the device: They also let attackers bypass security standards such as FIDO2.

According to The Register, as of the researchers' disclosure of the flaws to Samsung in May 2021, nearly 100 million Samsung Galaxy phones were jeopardized. Threatpost has reached out to Samsung to verify that estimate.

Samsung responded to the academics' disclosure by issuing a patch for affected devices that addressed CVE-2021-25444: an IV reuse vulnerability in the Keymaster Trusted Application (TA) that runs in the TrustZone. Keymaster TA carries out cryptographic operations in the Secure world via hardware, including a cryptographic engine. The Keymaster TA uses blobs, which are keys "wrapped" (encrypted) via AES-GCM. The vulnerability allowed for decryption of custom key blobs.

Then, in July 2021, the researchers revealed a downgrade attack – one that lets attacker trigger IV reuse vulnerability with privileged process. Samsung issued another patch – to address CVE-2021-25490 – that remoged the legacy blob implementation from devices including Samsung's Galaxy S10, S20 and S21 phones.

The Problem with Designing in the Dark

It's not just a problem with how Samsung implemented encryption, the researchers said. These problems arise from vendors – they called out Samsung and Qualcomm – keeping their cryptography designs close to the vest, the Tel Aviv U. team asserted.

"Vendors including Samsung and Qualcomm maintain secrecy around their implementation and design of TZOSs and TAs," they wrote in their paper's conclusion.

"As we have shown, there are dangerous pitfalls when dealing with cryptographic systems. The design and implementation details should be well audited and reviewed by independent researchers and should not rely on the difficulty of reverse engineering proprietary systems."

'No Security in Obscurity'

Mike Parkin, senior technical engineer at enterprise cyber risk remediation SaaS provider Vulcan Cyber, told Threatpost on Wednesday that getting cryptography right isn't exactly child's play. It's " a non-trivial challenge," he said via email. "It is by nature complex and the number of people who can do proper analysis, true experts in the field, is limited.

Parkin understands the reasons cryptologists push for open standards and transparency on how algorithms are designed and implemented, he said: "A properly designed and implemented encryption scheme relies on the keys and remains secure even if an attacker knows the math and how it was coded, as long as they don't have the key."

The adage "there is no security in obscurity" applies here, he said, noting that the researchers were able to reverse engineer Samsung's implementation and identify the flaws. "If university researchers could do this, it is certain that well-funded State, State sponsored, and large criminal organizations can do it too," Parkin said.

John Bambenek, principal threat hunter at the digital IT and security operations company Netenrich, joins Parkin on the "open it up" side. "Proprietary and closed encryption design has always been a case study in failure," he noted via email on Wednesday, referring to the "wide range of human rights abuses enabled by cell phone compromises," such as those perpetrated with the notorious Pegasus spyware.

"Manufacturers should be more transparent and allow for independent review," Bambenek said.

While most users have little to worry about with these (since-patched) flaws, they "could be weaponized against individuals who are subject to state-level persecution, and it could perhaps be utilized by stalkerware," he added.

Eugene Kolodenker, staff security intelligence engineer at endpoint-to-cloud security company Lookout, agreed that best practice dictates designing security systems "under the assumption that the design and implementation of the system will be reverse-engineered."

The same goes for the risk of it being disclosed or even leaked, he commented via email to Threatpost.

He cited an example: AES, which is the US standard of cryptography and accepted for top-secret information, is an open specification. "This means that the implementation of it is not kept secret, which has allowed for rigorous research, verification, and validation over the past 20 years," Kolodenker said.

Still, AES comes with many challenges, he granted, and "is often done incorrectly."

He thinks that Samsung's choice to use AES was a good decision. Unfortunately, the company "did not fully understand how to do so properly."

An audit of the whole system "might have prevented this problem," Kolodenker hypothesized.

Source: https://threatpost.com/samsung-shattered-encryption-on-100m-phones/178606/

13. The Wearable Future Is Hackable. Here's What You Need To Know

Quick mental math challenge: How many Apple Watches can you buy with $118 billion dollars? If you guessed around 296 million watches congrats, you're smarter than the writer of this blog! We had to use a calculator. The point is that's the predicted size of the US wearable market by 2028 according to a recent report. That means for as much wearable tech as we have in our lives already, even more, is on the way.

If you own a piece of wearable tech it's easy to understand why it's so popular. After all, it can track our fitness, provide contextual help in daily life, and, in the case of hearing aids, even do cool things like sync with Bluetooth. As VR and AR gains a foothold who knows what other incredible tech might be headed our way by 2028? However wearable tech also comes with certain risks. The most prominent: cybercriminals potentially gaining access to your data.

How can criminals gain access to your wearable data?

The weakest link in the wearables space is your mobile phone, not the actual wearable device itself. That's because wearables tend to link to your mobile device over a short-range wireless spectrum known as "Bluetooth." This spectrum is used to send and receive data between your wearable device and your mobile. That makes your mobile a prime target for hackers.

Most commonly, hackers gain access to the data on your mobile through malware-laden apps. These apps are oftentimes designed to look like popular apps, but with enough differences that they don't flag copyright suspicion.

What are they doing with my wearable data?

Hackers can use these malicious apps to do a variety of things from making phone calls without your permission, sending and receiving texts, and extracting personal information— all potentially without your knowledge. They can also, with the help of your wearable, track your location through GPS and record any health issues you've entered into your wearable. The point is: once they have permissions to your mobile device, they have a lot of control and a lot of resources.

The hacker can then use this data to conduct varying forms of fraud. Need a special prescription from your doctor that happens to sell well on the black market? Well, so does the hacker. Going out for a jog in the morning? Good information for a burglar to know. These personal details just scratch the surface of information available for the taking on your mobile devices.

Beyond wearables and into the internet of things

These types of threats aren't limited to wearables, however. The Internet of Things—the phenomenon of devices connected to the Internet for analysis and optimization—encompasses all sorts of other electronic devices such as washing machines and refrigerators that can put your data at risk as well. But these life-changing devices can be secured through education and industry standards. Two things we're working on day and night.

Defend your wearables and your personal information

- **Use a PIN.** All of your mobile devices ought to have a personal identification number (PIN). This basic security method is a great way of dissuading casual hackers or thieves from stealing your data.
- **Limit what you share.** Most wearables don't need access to every piece of information about you. You can lessen the likelihood of your wearable sharing sensitive information by only entering the information your wearable device requires. On the flip side, always double-check the permissions that the wearables app is requesting on your mobile device. Does it really need access to your location, camera roll, and address book? If not, be sure to alter these settings appropriately.
- **Use identity protection.** Identity protection can monitor your accounts online – accounts tied to your wearable – so you can receive alerts if that information has been compromised or found online. If it has, a service like McAfee's Identity Protection Service may also provide insurance and loss remediation as well.

Source: https://www.mcafee.com/blogs/privacy-identity-protection/hacking-wearable-devices/

14. Ransomware gangs, hackers pick sides over Russia invading Ukraine

Hacker crews are picking sides as the Russian invasion into Ukraine continues, issuing bans and threats for supporters of the opposite side.

This week, an administrator of the database sharing and marketplace Raidforums announced that it would close its door on users connecting from Russia, clearly expressing their position against Kremlin's actions.

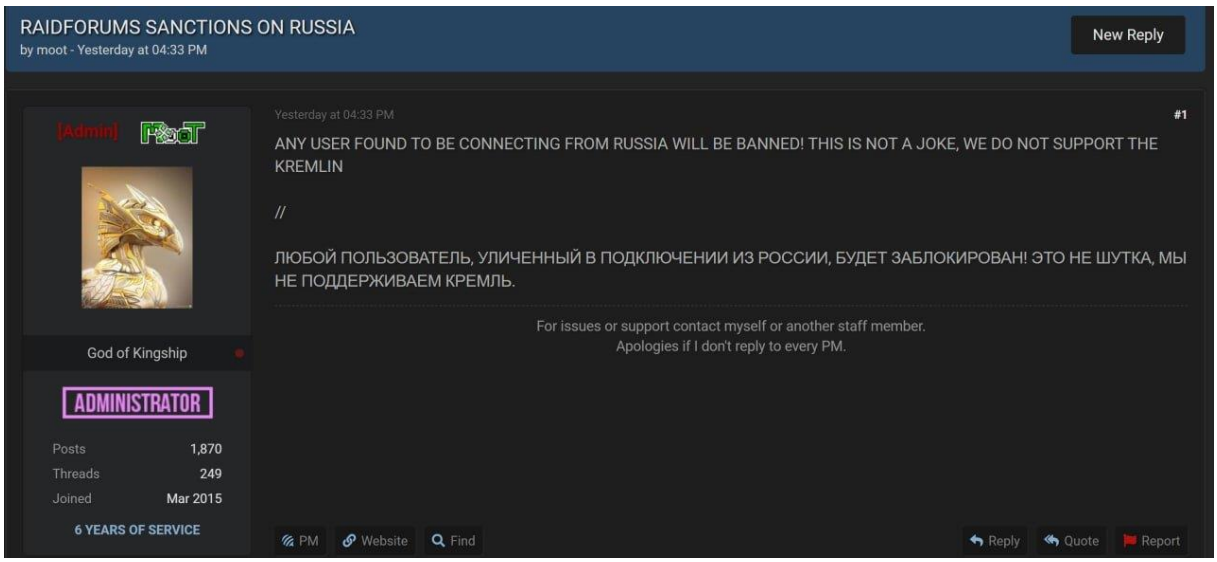
Earlier today, the Conti ransomware group stated their “full support of Russian government” and threatened with cyberattacks against anyone launching attacks against Russia.

Hackers react

Hackers, state-backed or not, have already launched cyberattacks, most of them against Ukrainian targets [1, 2, 3], with some targets in Russia also being hit [1].

With the Russian aggression continuing, the hacker community started to get more involved and express their stance in the conflict.

Following the political model of the U.S. and the EU, Raidforums published a notification yesterday saying that it would impose its own sanctions by banning any user connecting from Russia.



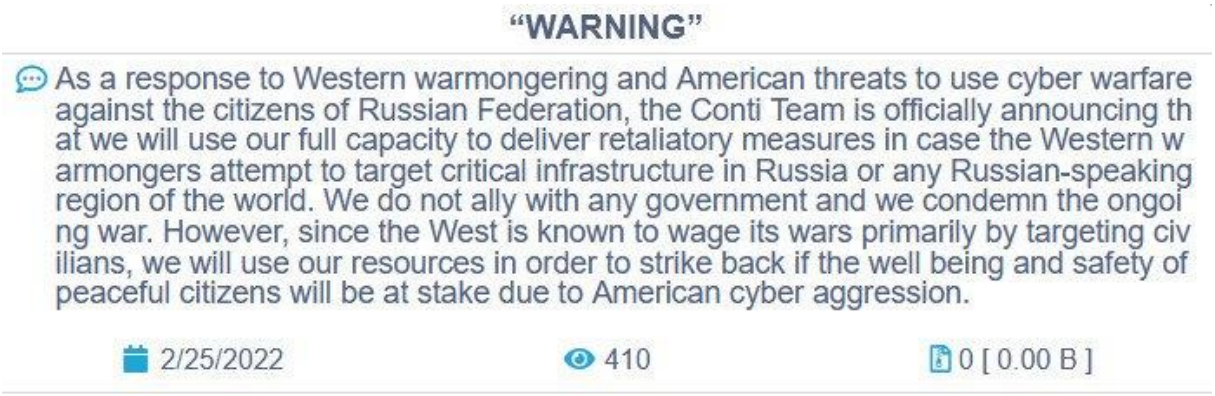
One member of the Raidforums community published a more abrasive message as a warning to "Russians." The user posted a database with emails and hashed passwords for the FSB.ru domain of Russia's main security agency, the Federal Security Service (FSB).

In the sample data shared on the forum as proof of provenance there are email addresses for FSB offices (directorates) in various regions.

Ransomware gangs get involved

Today, the Conti ransomware gang issued a warning that they would respond to cyber activity against Russia using all their resources “to strike back at the critical infrastructures of an enemy.”

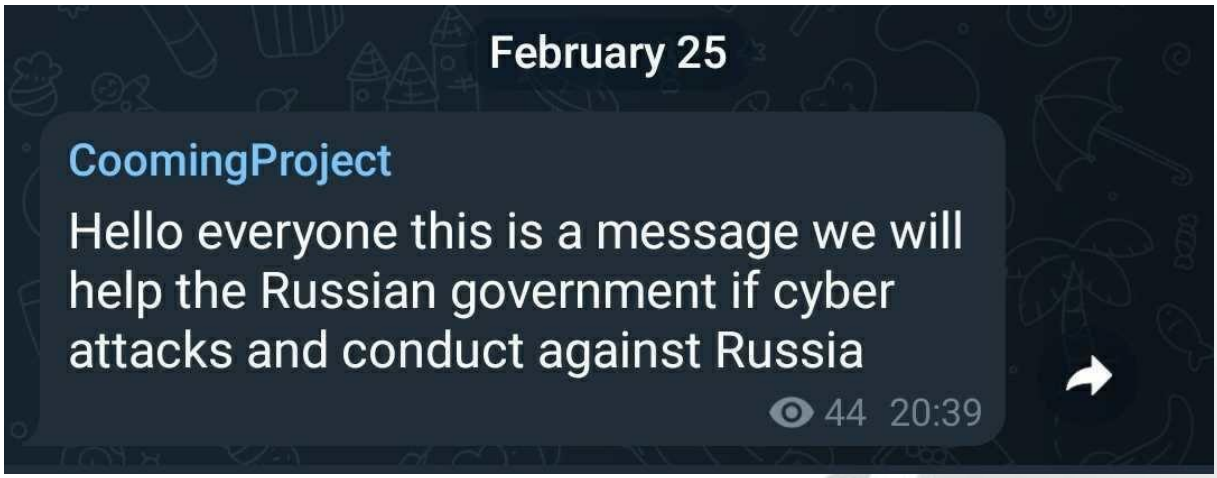
The gang changed their message about an hour later, saying that they "do not ally with any government and we condemn the ongoing war" but will respond to Western cyber aggression on Russian critical infrastructure.



Conti is one of the most active ransomware actors in the industrial sector, being responsible last year for breaching 63 companies operating industrial control systems (ICS), most of the in the manufacturing sector.

Conti also took control of BazarBackdoor, the stealthy malware developed by the TrickBot gang for compromising high-value targets.

CoomingProject, another, less known, ransomware group also announced their support for the Russian government if cyberattacks are aimed at the country.



h/t Valery Marchive

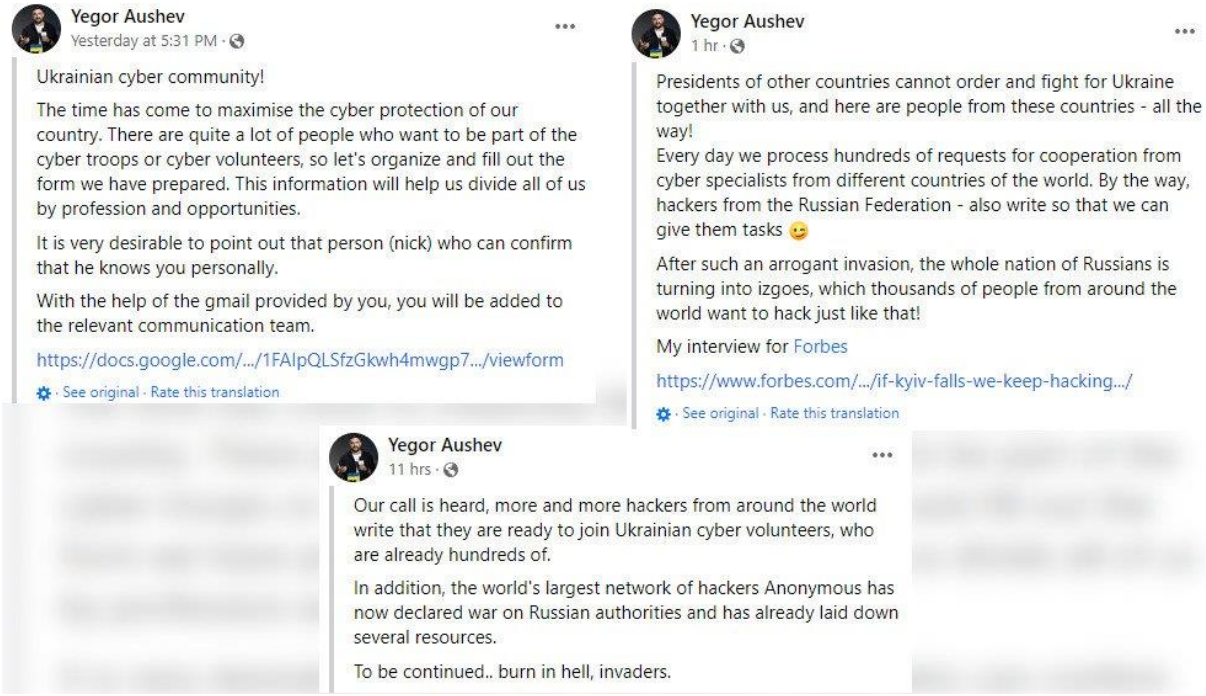
Ukraine asks hacker community for help

It appears that the Ukrainian side is also trying to engage its hacker force to defend critical infrastructure from coordinated cyberattacks and to carry out cyberespionage operations on Russian activity.

Reuters details that a message for the Ukrainian underground hacker community posted at the request of the Defense Ministry called the cybercommunity to enroll in a mission to defend the country.

The call to action was published through Yegor Aushev, the founder of Cyber Unit Technologies, who yesterday shared an application form for volunteer hackers to sign up declaring their skills for a better organization of tasks.

In one post, Aushev claims that even hackers around the world, including from Russia, have responded to his call, who will be grouped into teams for offensive and defensive action.



It is clear that modern warfare has entered a new age as physical armed forces are now openly supported by cyber activity carried not just by individuals with formal training but also self-taught hackers on both sides of the law.

Source: https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/

15. TrickBot malware operation shuts down, devs move to BazarBackdoor

The TrickBot malware operation has shut down after its core developers move to the Conti ransomware gang to focus development on the stealthy BazarBackdoor and Anchor malware families.

TrickBot is a notorious Windows malware infection that has dominated the threat landscape since 2016.

The malware is commonly installed via malicious phishing emails or other malware, and will quietly run on a victim's computer while it downloads modules to perform different tasks.

These modules perform a wide range of malicious activities, including stealing a domain's Active Directory Services database, spreading laterally on a network, screen locking, stealing cookies and browser passwords, and stealing OpenSSH keys.

TrickBot also has a long relationship with ransomware operations who partnered with the TrickBot group to receive initial access to networks infected by the malware.

In 2019, the TrickBot Group partnered with the Ryuk ransomware operation to provide the ransomware gang initial access to networks. In 2020, the Conti ransomware group, believed to be a rebrand of Ryuk, also partnered with TrickBot for initial access.

In 2021, TrickBot attempted to launch their own ransomware operation called Diavol, which has never really picked up steam, possibly because one of its developers was arrested.

Despite numerous takedown attempts by law enforcement, TrickBot had successfully rebuilt its botnet and continued to terrorize Windows networks.

That is until December 2021, when TrickBot distribution campaigns suddenly ceased.

TrickBot operation shuts down

Over the last year, Conti has become one of the most resilient and lucrative ransomware operations, responsible for numerous attacks on high-profile victims and amassing hundreds of millions of dollars in ransom payments.

As reported by BleepingComputer last week, due to the enormous wealth and capital at their disposal and TrickBot primarily being used by Conti, the ransomware gang slowly took control of the operation.

However, Conti did not recruit these "elite developers and managers" to work on the TrickBot malware, but rather to work on the more stealthy BazarBackdoor and Anchor malware families as seen by internal conversations shared with BleepingComputer by cybersecurity firm AdvIntel.

AdvIntel explained last week that the shift in development is because the TrickBot malware is too easily detected by security software and that the operation would be shut down shortly.

Yesterday, AdvIntel CEO Vitali Kremez told BleepingComputer that the TrickBot Group shut down all of the infrastructure for the TrickBot malware operation.

In a conversation with Kremez, BleepingComputer was told that the Conti ransomware now controls the TrickBot Group's malware development for their own needs.

With this shutdown, Kremez explained that TrickBot crime ring, who initially launched to pursue fraud, now focuses almost entirely on ransomware and breaching networks.

A report released yesterday by cyber intelligence firm Intel471 also confirmed that the operation was shutting down in favor of more profitable platforms.

While it is always good to see a malware operation shut down, the reality is that the ransomware gangs have already transitioned over to the more stealthy BazarBackdoor family.

BazarBackdoor has already seen increased distribution via email over the past six months, but with TrickBot's shutdown, we will likely see it become more prevalent in network breaches of corporate entities.

Source: https://www.bleepingcomputer.com/news/security/trickbot-malware-operation-shuts-down-devs-move-to-bazarbackdoor/

16. Xenomorph Malware Burrows into Google Play Users, No Facehugger Required

Researchers discovered a new, modular banking trojan with ties to Cerberus and Alien that has the capability to become a much larger threat than it is now.

An Android trojan dubbed Xenomorph has nested in Google Play, already racking up more than 50,000 downloads from the official app store, researchers warned. For anyone who downloaded the "Fast Cleaner" app, it's time to nuke it from orbit.

According to a ThreatFabric analysis, Xenomorph has a target list of 56 different European banks, for which it provides convincing facsimiles of log-in pages whenever a victim attempts to log into a mobile banking app. The goal of course is to steal any credentials that victims enter into the faux log-in overlay.

However, the malware is also a flexible, modular banking trojan, which has code overlaps and other ties to the Alien malware – hence the name. It notably contains the ability to abuse Android's accessibility services for broad control over a device's capabilities, which could open the door to dangerous features that go beyond hijacking mobile banking credentials.

"The Accessibility engine powering this malware, together with the infrastructure and command-and-control (C2) protocol, are carefully designed to be scalable and updatable," the researchers warned in a Monday posting. "The information stored by the logging capability of this malware is very extensive, and if sent back to the C2 server, could be used to implement keylogging, as well as collecting behavioral data on victims and on installed applications, even if they are not part of the list of targets."

That advanced functionality is not yet implemented, so the researchers have deemed Xenomorph as still under development. However, they noted that it's already making a mark on the banking trojan front: "Xenomorph is already sporting effective overlays [for banking apps] and being actively distributed on official app stores."

It also uses SMS and notification-interception to log and use potential two-factor authentication (2FA) tokens, according to ThreatFabric. And, they added, "It would be unsurprising to see this bot sport semi-automatic transfer system (ATS) capabilities in the very near future."

ATS is the process of automatically initiating wire transfers from the victims without needing to use credentials, thus bypassing 2FA and all anti-fraud measures.

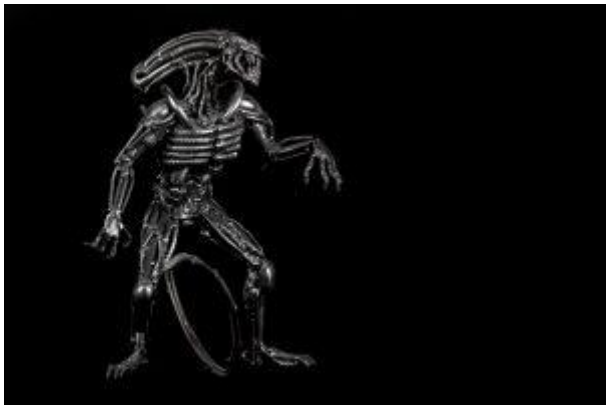
ThreatFabric observed the malware being loaded by a dropper hiding in a Google Play application called "Fast Cleaner" (since reported to Google). Sporting 50,000 installations, it purported to remove unused clutter and battery optimization blocks for better device processing times.

"This is not an uncommon lure, and we have seen malware families like Vultur and Alien being deployed by such application[s]," the researchers said.

Inside the Shell: Xenomorph's Core Functionality

In terms of its main overlay attack vector, Xenomorph is powered by Accessibility Services privileges, the researchers found.

"Once the malware is up and running on a device, its background services receive Accessibilty events whenever something new happens on the device," they explained in a Monday posting. "If the application opened is part of the list of targets, then Xenomorph will trigger an overlay injection and show a WebView Activity posing as the targeted package."



More specifically, once installed, the malware enumerates and sends back a list of installed packages on the infected device. Based on what targeted applications are present, it goes on to download the corresponding overlays to inject.

"The list of overlay targets returned by Xenomorph includes targets from Spain, Portugal, Italy and Belgium, as well as some general purpose applications like emailing services, and cryptocurrency wallets," according to ThreatFabric.

After obtaining Accessibility Services privileges, Xenomorph will first register and verify itself with the C2, by sending a request using the legitimate, open-source project Retrofit2 (a type-safe REST client for Android, Java and Kotlin developed by Square).

That first message contains the initial information exfiltrated about the device, according to ThreatFabric. After that, Xenomorph periodically polls for new commands from the C2.

For now, the commands allow the malware to log SMS messages, list the web injects sent by the C2, enable or disable intercept notifications, and enumerate installed apps.

Meanwhile, the malware also performs the aforementioned logging: "All the information gathered is only displayed on the local device logs, but in the future a very minor modification would be enough to add keylogging and Accessibility logging capabilities to the malware," researchers warned.

Part of the Alien Franchise?

ThreatFabric's analysis uncovered evidence of code reuse that links Xenomorph to the known Alien malware, which is a descendent of the infamous Cerberus malware.

These include the "use of the same HTML resource page to trick victims into granting the Accessibility Services privileges." And further, Xenomorph uses state-tracking through the use of the "SharedPreferences" file.

"This file is commonly used to track the state of an application," researchers noted. "However, the style of variable naming used by Xenomorph is very reminiscent of Alien, despite being potentially even more detailed."

They added, "potentially the most interesting fact is the actual name of the sharedPreferences file used to store the configuration for Xenomorph: the file is named ring0.xml. This might look like any other generic random string, but it happens to coincide with the name of the supposed actor behind the development of the original Alien malware."

Even though for now Xenomorph is a fairly typical banking trojan, ThreatFabric noted that it does have untapped potential.

"Modern banking malware is evolving at a very fast rate, and criminals are starting to adopt more refined development practices to support future updates," researchers concluded. "Xenomorph is at the forefront of this change…ThreatFabric predicts that with some more time to finish development, this malware could reach higher threat levels, comparable to other modern Android banking trojans."

Source: https://threatpost.com/xenomorph-malware-google-play-facehugger/178563/

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