



Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

July 2020

This security bulletin is powered by Telelink's 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!

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	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation	Vulnerability Analysis				
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.	Fake ransomware decryptor double-encrypts desperate victims' files	4
2.	Eavesdropping on Sound Using Variations in Light Bulbs.....	7
3.	Theft of CIA's 'Vault 7' Secrets Tied to 'Woefully Lax' Security	8
4.	Bank Card "Master Key" Stolen	10
5.	Nigerian entrepreneur pleaded guilty to \$11M Caterpillar fraud.....	10
6.	Microsoft Defender ATP can now protect Linux, Android devices.....	12
7.	Fxmisp hackers made \$1.5M selling access to corporate networks.....	14
8.	Visibility and Threat Detection in a Remote Working World	18
9.	Admin of carding portal behind \$568M in losses pleads guilty.....	22
10.	COVID-19 'Breach Bubble' Waiting to Pop?	25
11.	Business giant Xerox allegedly suffers Maze Ransomware attack.....	28
12.	UCSF Pays \$1.14M After NetWalker Ransomware Attack	31
13.	New Phishing scam targets website owners with free DNSSEC offer.....	33
14.	The Modern Workplace: Keeping Remote Workers Productive and Secure.....	37
15.	Microsoft releases urgent security updates for Windows 10 Codecs bugs.....	41

1. Fake ransomware decryptor double-encrypts desperate victims' files

A fake decryptor for the STOP Djvu Ransomware is being distributed that lures already desperate people with the promise of free decryption. Instead of getting their files back for free, they are infected with another ransomware that makes their situation even worse.

While ransomware operations such as Maze, REvil, Netwalker, and DoppelPaymer get wide media attention due to their high worth victims, another ransomware called STOP Djvu is infecting more people than all of them combined on a daily basis.

With over 600 submissions a day to the ID-Ransomware ransomware identification service, STOP ransomware is the most actively distributed ransomware over the past year.



STOP Djvu ransomware submissions to ID-Ransomware

Emsisoft and Michael Gillespie had previously released a decryptor for older STOP Djvu variants, but newer variants cannot be decrypted for free.

If the ransomware is so common, you may be wondering why it doesn't get much attention?

The lack of attention is simply because the ransomware mostly affects home users infected through adware bundles pretending to be software cracks.

While downloading and installing cracks is not excusable, many of those who are infected simply cannot afford to pay a \$500 ransom for a decryptor.

Double-encrypting someone's data with a second ransomware is just kicking someone while they are already down.

Zorab double-encrypts a victim's data

Unfortunately, this is what a new ransomware called Zorab discovered by MalwareHunterTeam is doing.

The creators of the Zorab ransomware have released a fake STOP Djvu decryptor that does not recover any files for free but instead encrypts all of the victim's already encrypted data with another ransomware.



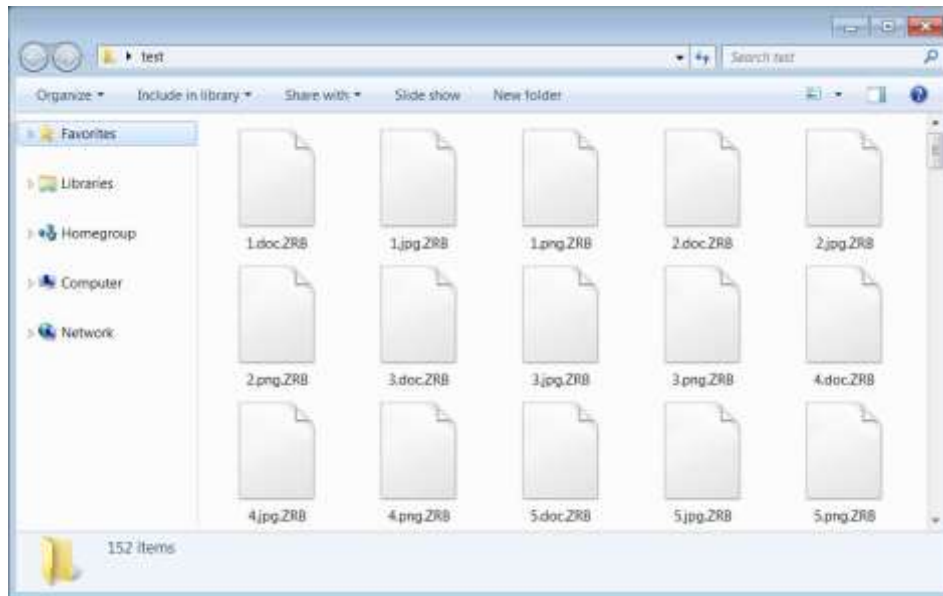
Fake STOP Djuv decryptor

When a desperate user enters their information in the phony decryptor and clicks on 'Start Scan,' the program will extract another executable called crab.exe and saves it to the %Temp% folder.

```
private void button1_Click(object sender, EventArgs e)
{
    let num1;
    let num2;
    try
    {
        T1_011;
        ProjectData.ClearProjectData();
        num = -2;
        T1_011;
        let num0 = 2;
        this.button1.Enabled = true;
        T1_011;
        num2 = 3;
        this.button1.Text = "Decrypt";
        T1_011;
        num1 = 4;
        File.WriteAllBytes(Path.Combine(Path.GetTempPath(), "crab.exe"), Resources.crab);
        T1_011;
        num2 = 5;
        Process.Start(Path.Combine(Path.GetTempPath(), "crab.exe"));
        T1_011;
        num1 = 0;
        ToolStrip1.Focus();
        T1_011;
        goto T1_0C1;
        T1_0B1;
        let arg_70_0 = num1 + 1;
        num2 = 0;
        Push(ISharpCode.Decompiler.ILAct.ILLabel[], arg_70_0);
        T1_011;
        goto T1_011;
        num1 = num2;
        Push(ISharpCode.Decompiler.ILAct.ILLabel[], (num + -2) ? num : 1);
        T1_011;
        goto T1_011;
    }
    object arg_H1_0;
    bool filter(arg_H1_0 is Exception & num != 0 & num2 == 0);
    T1_011;
    throw ProjectData.CreateProjectError(-2146828217);
    T1_0C1;
    if (num1 != 0)
    {
        ProjectData.ClearProjectData();
    }
}
```

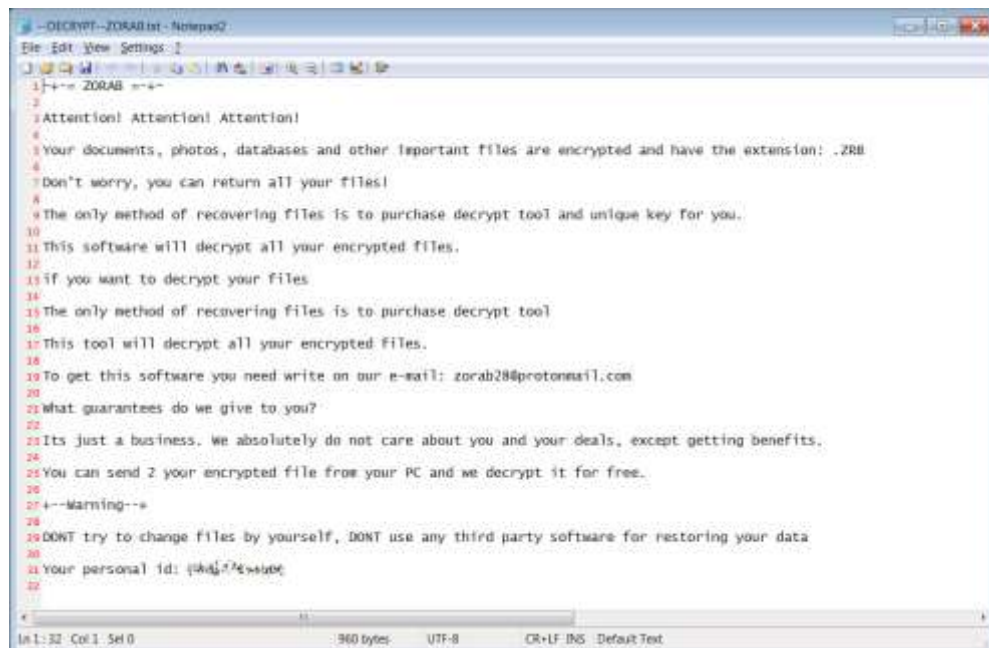
Extracting and executing the crab.exe program

Crab.exe is another ransomware called Zorab, which will begin to encrypt the data on the computer. When encrypting files, the ransomware will append the .ZRB extension to the file's name.



Zorab encrypted files

The ransomware will also create ransom notes named '--DECRYPT--ZORAB.txt.ZRB' in each folder that a file is encrypted. This note contains instructions on how to contact the ransomware operators for payment instructions.



Zorab ransom note

This ransomware is currently being analyzed, and users should not pay the ransom until it is confirmed no weakness can be used to recover Zorab encrypted files for free.

Source: <https://www.bleepingcomputer.com/news/security/fake-ransomware-decryptor-double-encrypts-desperate-victims-files/>

2. Eavesdropping on Sound Using Variations in Light Bulbs

New research is able to recover sound waves in a room by observing minute changes in the room's light bulbs. This technique works from a distance, even from a building across the street through a window.

Details:

In an experiment using three different telescopes with different lens diameters from a distance of 25 meters (a little over 82 feet) the researchers were successfully able to capture sound being played in a remote room, including The Beatles' *Let It Be*, which was distinguishable enough for Shazam to recognize it, and a speech from President Trump that Google's speech recognition API could successfully transcribe. With more powerful telescopes and a more sensitive analog-to-digital converter, the researchers believe the eavesdropping distances could be even greater.

It's not expensive: less than \$1,000 worth of equipment is required. And unlike other techniques like bouncing a laser off the window and measuring the vibrations, it's completely passive.

Source: https://www.schneier.com/blog/archives/2020/06/eavesdropping_o_9.html

3. Theft of CIA's 'Vault 7' Secrets Tied to 'Woefully Lax' Security

An internal investigation into the 2016 CIA breach condemned the agency's security measures, saying it "focused more on building up cyber tools than keeping them secure."

A just-released report on the 2016 Central Intelligence Agency (CIA) data breach, which led to the Vault 7 document dump on WikiLeaks, blames "woefully lax" security by the nation's top spy agency.

The conclusions were part of an internal 2017 Department of Justice (DoJ) report on the CIA breach. On Tuesday, Sen. Ron Wyden released portions of the report (PDF) that were made public via recent DoJ court filings.

The report described the CIA as "focused more on building up cyber tools than keeping them secure." Part of the investigation revealed sensitive cyber weapons were not compartmented and government cybersecurity researchers shared systems administrator-level passwords. Systems with sensitive data were not equipped with user activity monitoring and historical data was available to users indefinitely, the report stated.

"In a press to meet growing and critical mission needs, [the CIA's Center for Cyber Intelligence (CCI) arm] had prioritized building cyber weapons at the expense of securing their own systems," according to the report. "Day-to-day security practices had become woefully lax."

At least 180 gigabytes (up to as much as 34 terabytes of information) was stolen in the breach, the report said – roughly equivalent to 11.6 million to 2.2 billion electronic document pages. The data stolen included cyber tools that resided on the CCI's software development network (DevLAN). The mission of the CCI, which was targeted by the data breach, is to "transform intelligence" through cyber operations.

The report outlined various security issues discovered in the CCI. For instance, while CCI's DevLAN network had been certified and accredited, CCI had not worked to develop or deploy user activity monitoring or "robust" server audit capabilities for the network, according to the report.

Because of that lack of user activity monitoring and auditing, "we did not realize the loss had occurred until a year later, when WikiLeaks publicly announced it in March 2017" by leaking troves of stolen CIA hacking tools, according to the report. It said, if the data had not published, the agency might still be unaware of the loss.

"Furthermore, CCI focused on building cyber weapons and neglected to also prepare mitigation packages if those tools were exposed," according to the report. "These shortcomings were emblematic of a culture that evolved over years that too often prioritized creativity and collaboration at the expense of security."

Another issue is that the agency lacked “any single officer” tasked with ensuring that IT systems were built secure and remained so throughout their lifecycle. Because no one had that task, no one person was held accountable for the breach, the report said. And, there was no lookout for “warning signs” that insiders with access to CIA data posed a risk.

According to The Washington Post, which broke news of the report, the task force’s report is being used as evidence in the trial of former CIA employee Joshua Schulte, who has been accused of stealing the CIA’s hacking tools and giving them to WikiLeaks.

The report outlined several (heavily redacted) recommendations for the agency to take to bolster its security. That includes enhancing its security guidelines and classified information handling restrictions for zero-day exploits and offensive cyber tools.

However, Sen. Wyden, a member of the Senate Intelligence Committee, said in a stinging public letter to John Ratcliffe, the director of National Intelligence, that even three years later the U.S. intelligence community still has a ways to go in improving its security practices.

For instance, he said, the intelligence community has yet to protect its .gov domain names with multi-factor authentication; and, the CIA, National Reconnaissance Office and National Intelligence office have yet to enable DMARC anti-phishing protections, he said.

“Three years after that report was submitted, the intelligence community is still lagging behind, and has failed to adopt even the most basic cybersecurity technologies in widespread use elsewhere in the federal government,” he said. “The American people expect you to do better, and they will then look to Congress to address these systematic problems.”

Fausto Oliveira, principal security architect at Acceptto, told Threatpost that Wyden is “quite right” in asking why standard security practices in the industry are not being adopted by the CIA.

“Based on the findings of the report, it appears that there was a lack of IT and cybersecurity governance that led to a lax adoption of security controls,” he said. “It is not an operational matter, it is a matter of the agency’s management not setting the right goals to manage the risks associated with operating an organization, specifically an organization that is a desirable target for all kinds of attackers.”

Source: <https://threatpost.com/theft-of-cias-vault-7-secrets-tied-to-woefully-lax-security/156591/>

4. Bank Card "Master Key" Stolen

South Africa's Postbank experienced a catastrophic security failure. The bank's master PIN key was stolen, forcing it to cancel and replace 12 million bank cards.

The breach resulted from the printing of the bank's encrypted master key in plain, unencrypted digital language at the Postbank's old data centre in the Pretoria city centre.

According to a number of internal Postbank reports, which the *Sunday Times* obtained, the master key was then stolen by employees.

One of the reports said that the cards would cost about R1bn to replace. The master key, a 36-digit code, allows anyone who has it to gain unfettered access to the bank's systems, and allows them to read and rewrite account balances, and change information and data on any of the bank's 12-million cards.

The bank lost \$3.2 million in fraudulent transactions before the theft was discovered. Replacing all the cards will cost an estimated \$58 million.

Source: https://www.schneier.com/blog/archives/2020/06/bank_card_maste.html

5. Nigerian entrepreneur pleaded guilty to \$11M Caterpillar fraud

Nigerian entrepreneur Obinwanne Okeke is facing 20 years in prison after pleading to conspiracy to commit wire fraud that caused US Fortune 100 corporation Caterpillar \$11 million in losses as part of a business email compromise (BEC) fraud scheme.

The defendant, also known as 'Invictus Obi', was listed by Forbes on a list of "Africa's 30 under 30" in 2016 after founding a group of companies known as Invictus Group involved in telecoms, construction, oil and gas, agriculture, and real estate.

"According to court documents, Obinwanne Okeke, 32, and other conspirators engaged in a conspiracy from approximately 2015 to 2019 to conduct various computer-based frauds," a Department of Justice press release says.

"The conspirators obtained and compiled the credentials of hundreds of victims, including victims in the Eastern District of Virginia and elsewhere."

How it all went down

Okeke and his conspirators were able to successfully defraud Unatrac Holding Limited, one of Caterpillar's export sales office, after sending a phishing email to Unatrac's Chief Financial Officer (CFO) and stealing his Microsoft Office 365 login credentials.

They later used his account for sending fraudulent wire transfer requests to Unatrac's financial team in the form of fake invoices and emails designed to look like they were sent by the CFO.

Okeke also added email filters to automatically mark legitimate emails as read and moved them out of the CFO's inbox to hide any replies he got from the recipients of the fraudulent wire transfer requests containing fake invoices.

"In June, 2018, representatives for Unatrac Holding Limited, the export sales office for Caterpillar heavy industrial and farm equipment, headquartered in the United Kingdom, contacted the FBI," an FBI affidavit issued in support of an arrest warrant and a criminal complaint against Okeke reads.

"They reported that Unatrac had been victimized through an email compromise, which ultimately resulted in fraudulent wire transfers totaling nearly \$11 million (11 million US Dollars)."

Proof is in the logs

After Unatrac's report and reviewing the documentation the company's representatives provided as proof of the fraudulent wire transfers, the FBI opened an investigation in July 2018.

During the investigation, they were able to link Okeke with multiple Gmail email addresses used throughout the fraud scheme with the help of a confidential source and login session cookies.

After analyzing server logs, an FBI agent also found that Okeke accessed the CFO's account 464 times between April 6 and April, 2018, mostly from Nigerian IP addresses.

An arrest warrant was issued in Okeke's name by the United States District Court for the Eastern District of Virginia in August 2019.

On June 18, 2020, Okeke pleaded guilty to a conspiracy to commit wire fraud and he will be sentenced on October 22 when he will be facing a maximum penalty of 20 years in prison.

Source: <https://www.bleepingcomputer.com/news/security/nigerian-entrepreneur-pleaded-guilty-to-11m-caterpillar-fraud/>

6. Microsoft Defender ATP can now protect Linux, Android devices

Microsoft Defender Advanced Threat Protection (ATP) has expanded to non-Windows platforms and is now generally available for enterprise customers using Linux devices and in public preview for those with Android devices.

"Adding Linux into the existing selection of natively supported platforms by Microsoft Defender ATP marks an important moment for all our customers," Microsoft said.

With the added announcement of the Microsoft Defender ATP for Android public preview, the company strives to provide a unified security solution for the most used server and desktop platforms used in enterprise environments.

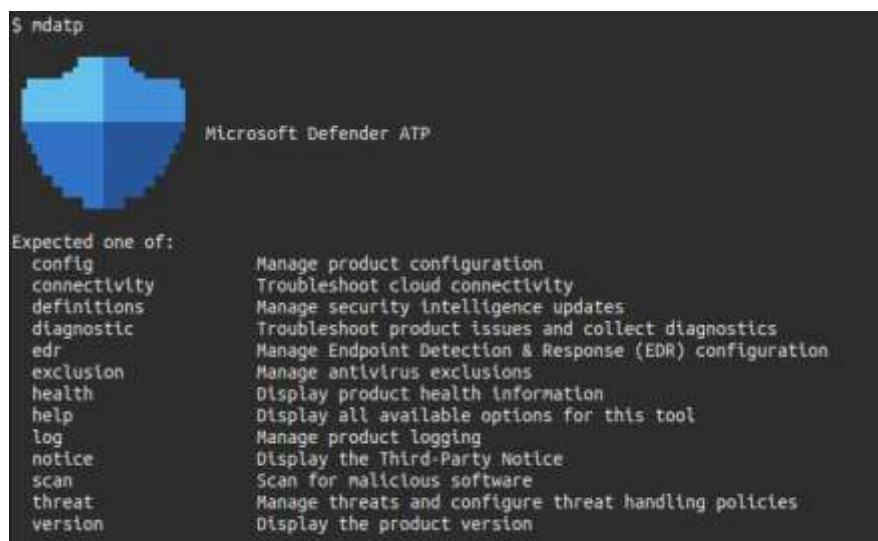
Generally available on most popular Linux distros

Microsoft Defender ATP for Linux was first showcased during the Ignite 2019 conference and entered public preview in February 2020, with support for several Linux server distributed versions.

On Linux endpoints, the Microsoft enterprise endpoint security solution comes in the form of a command-line product that sends all threats it detects to the Microsoft Defender Security Center.

Right now, Microsoft Defender ATP for Linux comes with support for recent versions of the most common Linux Server distributions including RHEL 7.2+, CentOS Linux 7.2+, Ubuntu 16 LTS or higher LTS, SLES 12+, Debian 9+, Oracle Linux 7.2.

Admins with a Microsoft Defender ATP for Servers license can deploy and configure it on Linux devices with the help of Puppet or Ansible, as well as with any existing Linux configuration management tool.



```
S ndatp
Microsoft Defender ATP

Expected one of:
config          Manage product configuration
connectivity    Troubleshoot cloud connectivity
definitions     Manage security intelligence updates
diagnostic      Troubleshoot product issues and collect diagnostics
edr            Manage Endpoint Detection & Response (EDR) configuration
exclusion        Manage antivirus exclusions
health          Display product health information
help            Display all available options for this tool
log             Manage product logging
notice          Display the Third-Party Notice
scan            Scan for malicious software
threat          Manage threats and configure threat handling policies
version         Display the product version
```

Microsoft Defender ATP for Linux (Microsoft)

Microsoft provides onboarding information on how to install, update, and configure it for admins that haven't previously enrolled in the public preview. Those already running the preview version only have to update the agent to version 101.00.75 or higher.

"This initial release delivers strong preventive capabilities, a full command-line experience on the client to configure and manage the agent, initiate scans, manage threats, and a familiar integrated experience for machines and alert monitoring in the Microsoft Defender Security Center," Microsoft explained.

Android public preview

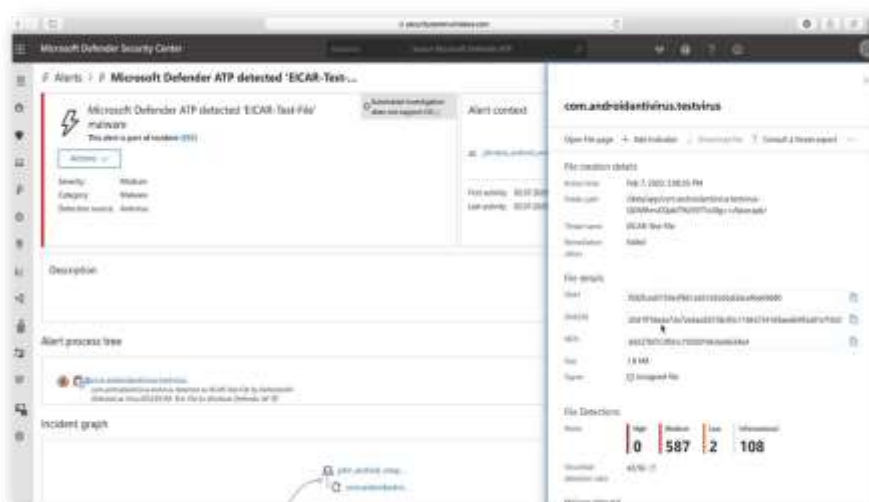
After previewing Microsoft Defender ATP for Android at RSA Conference 2020, Microsoft has now announced the public preview of mobile threat defense capabilities for Android devices.

"The public preview of Microsoft Defender ATP for Android will offer protection against phishing and unsafe network connections from apps, websites, and malicious apps," the company's announcement reads.

"In addition, the ability to restrict access to corporate data from devices that are deemed 'risky' will enable enterprises to secure users and data on their Android devices.

"All events and alerts will be available through a single pane of glass in the Microsoft Defender Security Center, giving security teams a centralized view of threats on Android devices along with other platforms."

At the moment, Microsoft Defender ATP for Android provides enterprise users with phishing protection, proactive scanning of potential malicious apps, files, and potentially unwanted applications (PUA), security breach defense, and a unified security experience through Microsoft Defender Security Center.



Android malware detection in Microsoft Defender Security Center (Microsoft)

Customers with preview features enabled can try out Microsoft Defender ATP for Android starting today(they can be toggled on from the Microsoft Defender Security Center).

More details about the Microsoft Defender ATP for Android public preview including installation, prerequisites, and system requirements are available here.

"In the coming months we will be releasing additional capabilities on Android and you will hear more from us about our investments in mobile threat defense for iOS devices as well," Microsoft 365 Security Corporate Vice President Rob Lefferts added.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-defender-atp-can-now-protect-linux-android-devices/>

7. Fxmsp hackers made \$1.5M selling access to corporate networks

New details have emerged on the activity of the infamous Fxmsp hacker that last year was advertising access to the networks of three cybersecurity vendors.

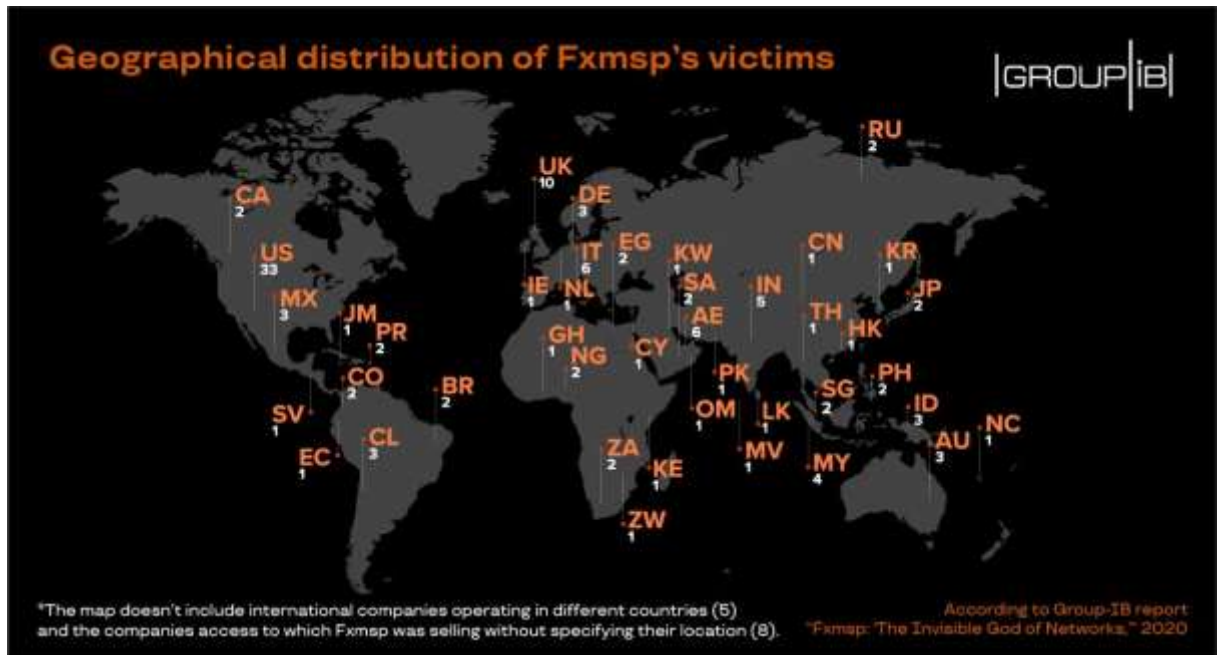
Researchers tracking Fxmsp's ventures on underground forums counted the network intrusions associated with this actor and revealed the presumed identity of the attacker.

Worldwide hacking activity

Fxmsp became widely known outside hacker forums about a year ago when cybersecurity boutique Advanced Intelligence (AdvIntel) published a series of reports on the actor's attempts to close a \$300,000 deal for selling access to networks belonging to Symantec, Trend Micro, and McAfee.

The actor and their accomplice slipped under the public radar soon after getting too much media attention, likely continuing activity over private messages.

Researchers at Group-IB examined Fxmsp's exposure in the public areas of the forums where they were advertising their business, assessing that the actor breached networks of at least 135 companies in 44 countries.



Among the targets are small and medium-sized enterprises (SME), government organizations, banks, and Fortune 500 companies. Group-IB's conservative estimate is that in 3+ years (since 2016) Fxmsp made at least \$1.5 million from selling network access.

In May 2019, AdvIntel assessed with high confidence that Fxmsp is a credible threat "with a history of selling verifiable corporate breaches returning them profit close to \$1,000,000."

This is not all the money, though, because transactions for access to 20% of the companies compromised were carried out in private and did not come with a public price tag.

Fxmsp stopped all their public activity in late 2019, Group-IB says, but not before advertising access to a power company in Europe that suffered a ransomware attack in 2020. One such company hit by ransomware this year is the Italian multinational Enel Group.

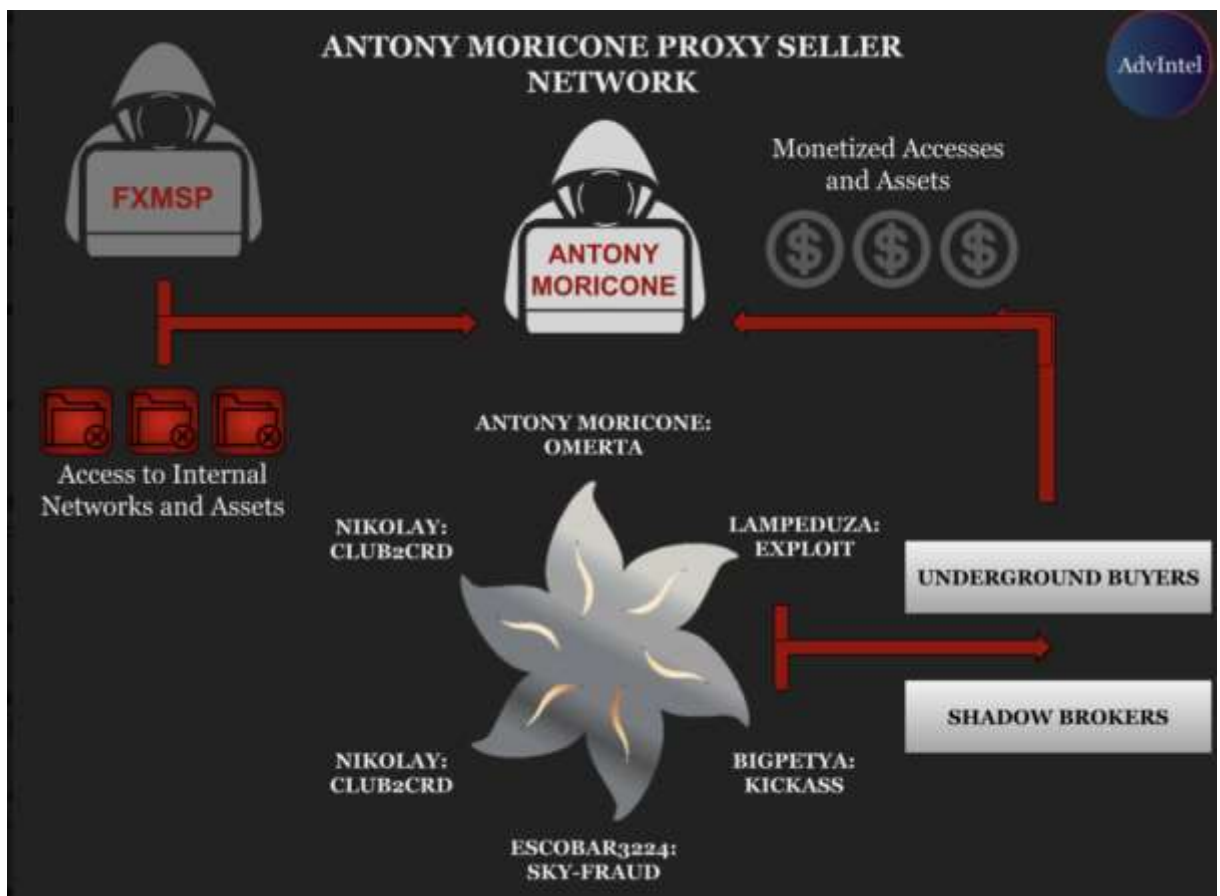
It may seem too big of a profit for hackers with little to no experience in marketing their assets. However, Fxmsp was not alone in this.

According to Yelisey Boguslavskiy, AdvIntel director of security research, Fxmsp was the hacking part of a crew (GPTitan) consisting of specialists "geared to secretly work in financial environments" to steal from high-profile networks data relevant to customers.

GPTitan was assisted in their work by two other crews, one in China and one in the U.S., a collaboration that led to the data breaches at the antivirus companies from the spring of 2019.

An independent source with knowledge about Fxmsp activity told BleepingComputer that the actor stopped acting alone and had expanded into a team.

The non-hacking part of Fxmsp was in charge of marketing and monetizing the network access and the data. A network of affiliates operating under the alias Antony Moricone offered to share breached information to hackers, financial shadow brokers, and 'grey' information traders who used it to shift to their advantage the decision-making process in companies they had an interest in.

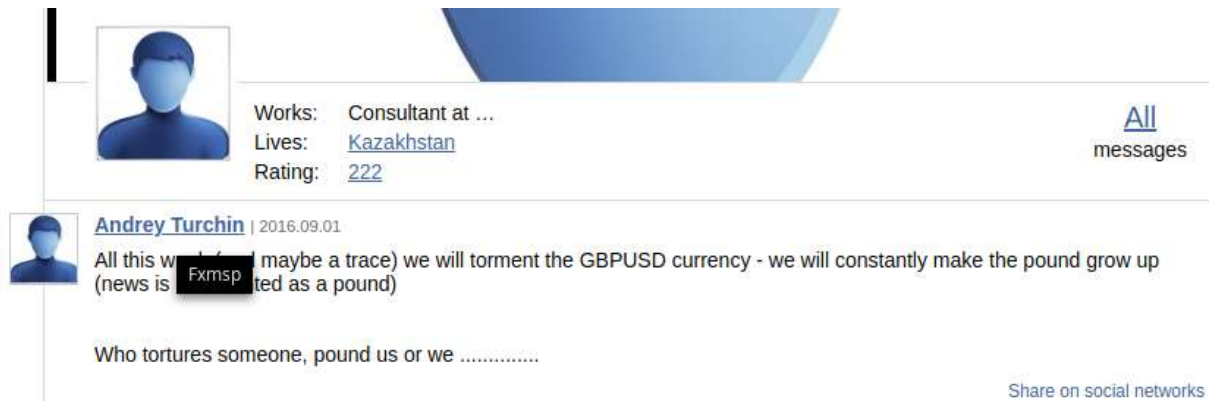


Boguslavskiy does not dismiss the possibility that the aliases in the Antony Moricone crew be operated by a single individual on multiple forums, which is what Group-IB states in their report:

"Group-IB experts were able to identify Lampeduza's nicknames on other forums: Antony Moricone, BigPetya, Fivelife, Nikolay, tor.ter, andropov, and Gromyko" - Group-IB

The name behind the alias

The researchers also revealed in a report today what may be the identity behind Fxmsp: Andrey Turchin (allegedly of Kazakhstan), the same as the one found by BleepingComputer in research last year.



Group-IB’s research, though was more comprehensive as it followed the breadcrumbs in forum posts from the actor and correlated them with domain name registration data and social media profiles on Russian networks (VK, My World).



Dmitry Volkov, CTO of Group-IB says about Fxmsp that they set a trend that led in the second half of 2019 to almost doubling the number of network access sellers specialized in corporate intrusions.

“Prior to Fxmsp joining the underground, the sellers would offer RDP access to separate servers, without even bothering to ensure persistence or performing reconnaissance in the network. Fxmsp took this service into a whole new level” - Dmitry Volkov

Volkov says that Fxmsp might still be active these days, keeping their business private. Even if they’re not on the scene anymore, they set an example for others.

According to trusted sources, Andrey was approached and possibly detained by Kazakhstan law enforcement. BleepingComputer has not been able to independently confirm this information.

Source: <https://www.bleepingcomputer.com/news/security/fxmsp-hackers-made-15m-selling-access-to-corporate-networks/>

8. Visibility and Threat Detection in a Remote Working World

At the outset of the COVID-19 pandemic, when governments around the world put stay-at-home orders in place, it was hard to imagine the state of work would permanently change. Yet, as organizations rapidly adopted and expanded systems to enable a remote workforce — which [doubled in size](#) in just three weeks — company cultures began shifting, too. As employees adjusted to life working remotely, many proved to their employers that productivity could remain high, and in some cases even increase, while they worked from home.

As a result of this forced experiment, many experts and executives now predict that flexible, work-from-home policies are here to stay. Research from Gartner suggests 41% of employees will continue to work from home, up from 30% before the pandemic, as reported by [ZDNet](#). Additionally, 13% of chief financial officers (CFOs) have already started to cut real estate expenses spent on office space. With remote work here to stay, security professionals need ways to maintain visibility, monitoring and threat detection when the network perimeter, which has been disintegrating for years, has become almost non-existent.

Despite the new blind spots, below are four key areas in which a centralized security information and event management (SIEM) solution can help security teams re-gain and increase visibility and monitoring controls.

Email

Targeted attackers are good at crafting compelling phishing emails and they're only getting better. Email is one of the most important threat vectors to monitor, as [94% of malware](#) that reaches an organization is delivered via phishing. To get early insights into these threats and, more importantly, be able to track exactly what happens after a phishing email is opened, security teams need a centralized view of what's happening across the organization.

To achieve this, security operations center (SOC) teams can send a combination of relevant email events and network flows to a centralized SIEM solution for analysis. By

ingesting and analyzing email events or email security events, such as those from Proofpoint or Cisco IronPort, security analysts can get a more effective, comprehensive view of email-based threats.

For deeper insight, analysts can also take advantage of [network analytics](#) to extract additional attributes, such as sender email, attachment name, file hash and URL and then correlate those attributes against threat intelligence in real time. As a result, this network-level insight can provide early [visibility and alerting](#) for known threats and suspicious attributes that may indicate a phishing attack.

Endpoint

Before the massive shift to remote working, there were typically two types of companies:

- Those who were almost entirely in-office, with users on desktops.
- Those who were remote-enabled, with users on laptops that could connect to the network via a VPN.

When workers went almost entirely remote, both faced challenges. In-office organizations needed to rapidly figure out how to enable core services and applications for remote workers and, in some cases, deploy a virtual private network (VPN) for the first time. Remote-enabled organizations saw massive spikes in VPN usage, overwhelming networks and dramatically reducing speed, essentially forcing users to work off the VPN to maintain productivity. From a security perspective, both situations introduced a massive blind spot for endpoint and user activity.

To regain visibility, security teams can leverage a combination of endpoint operating systems (OS), VPN and endpoint detection and response (EDR) events to help with threat detection. With native Windows, macOS and Linux logging, security teams can get insight into what's happening at the endpoint level. By augmenting Windows event logging with [Sysmon](#), teams can gain even deeper threat-relevant insights, such as process activity and domain name system (DNS) requests.

For organizations using an EDR solution, such as [Carbon Black](#) or [CrowdStrike](#), endpoint security events can be sent to a centralized SIEM solution and correlated against other enterprise data for end-to-end threat visibility. When EDR is tightly integrated with a SIEM, response actions can be initiated directly from the SIEM interface. Lastly, when users sign on to the VPN or go through [risk-based authentication](#) to access applications, these solutions can provide insight into the endpoint's location, MAC address, user agent and other valuable information that can provide insight into whether this is the real user.

Once this valuable data is collected in one place, security teams can apply a series of both [machine-learning](#) and [correlation-based](#) analytics to detect known and unknown

threats. For a security operations team, it's particularly useful to look for SIEM vendors who provide [pre-built security use cases](#) and analytics so you don't have to invest time and money in researching and developing these from scratch.

Application

Monitoring application activity should be a key focus for teams since, unlike with endpoints, organizations are still in control even off of the network. Application monitoring can also help to expose attackers who are already inside the network. Application monitoring can be enforced at a number of levels:

- At sign-on through identity as a service (IDaaS) solutions, such as [Cloud Identity Connect](#) or [Okta](#).
- From sign-on through to sign-off directly via applications such as SAP, Salesforce.com or [Office 365](#).
- Via a cloud access security broker (CASB) solution, such as Zscaler, to monitor who is accessing or attempting to access which applications.
- Directly within the application stack, including the OS [container orchestration](#) platforms (like Kubernetes), containers themselves and API calls within these environments.

In addition to monitoring and analyzing events at each of these levels, network monitoring can provide detailed insight into how application data is traversing the network, who and what is connecting to these systems and if any abnormal traffic has been witnessed. This added layer of insight can augment existing visibility and insight to help to uncover several suspicious activities faster, such as compromised accounts and lateral movement data exfiltration attempts. Further, network monitoring can be particularly helpful when attackers have gained enough control to successfully use detection evasion techniques, such as disabling logging. As a highly reliable source of truth, network data can show when systems and applications are still online even though they aren't sending logs, and it can also continue to provide visibility into what those systems and applications are doing.

Cloud

With many physical data centers temporarily closed, organizations have faced an urgent need to minimize the requirement of the on-site physical maintenance of IT systems. Many organizations have quickly accelerated the adoption of cloud infrastructures to support their workloads and applications to maintain business continuity. Since many of these migrations were already planned — just often for later timelines — most security teams should expect these investments are here to stay.

To gain earlier insights into risks and threats in these environments, security teams can monitor a range of events including user activity, application activity and resource and configuration changes. Fortunately, the major public cloud vendors, such as [AWS](#), [IBM](#), [Azure](#) and Google Cloud, provide a rich set of log, event and network [flow data](#) that can be brought into a centralized SIEM solution to gain visibility and detection across on-premises and multicloud environments.

By ingesting this data and applying security use cases to it, analysts can gain insight into several suspicious activities, such as:

- **Anomalous user and account activity**, such as abnormal authentication activity, multiple logins from different geographies or suspicious root user activity.
- **Anomalous workload activity**, including abnormal API calls, suspicious [container activity](#) or non-standard services accessing resources.
- **High-risk configuration changes**, such as suspicious IAM or security group policy changes, changes to S3 bucket policies or new or altered certificates.
- **Suspicious resource changes**, such as non-standard virtual private cloud (VPC) or EC2 instances or a rapid increase in the number or size of EC2 instances potentially indicative of [cryptocurrency mining](#).

While many of the cloud providers have their own native security capabilities, without a centralized view into security data across environments, analysts are forced to work within complex data silos. Today, [62% of public cloud adopters](#) use two or more public clouds, and, on average, organizations use a total of 4.8 separate public and private cloud environments. For an analyst struggling to keep up with an ever-growing workload, getting [centralized cloud visibility](#) combined with the ability to automatically analyze, detect and track threats as they progress through different environments, is critical. A centralized SIEM solution that's capable of ingesting and analyzing the event and flow data across cloud and on-premises environments can help analysts quickly and more effectively detect threats before they escalate and cause serious damage.

Putting it all together

As a result of the rapid shift to remote work, many IT organizations now have the technology to support remote employees. And over the last few months, employees have proven they can remain productive from home. As we move forward into a new normal, one clear change that is here to stay is more flexible, remote-friendly working policies. As a result, security operations teams need a sustainable, long-term strategy to maintain visibility and threat detection over a network that has new blind spots and hardly any remaining perimeter.

By doubling down on centralized security analytics, with a particular focus on phishing, endpoint, application and cloud security use cases, security analysts can gain new insights to compensate for lost visibility and ultimately help strengthen the security posture of their organizations. In this remote world when teams are already stretched thin, consider SIEM solutions that can run anywhere, including as SaaS or in a public cloud, offer pre-built use cases to make detection easier and improve overall value and offer tight integrations with SOAR solutions, such as [Resilient](#), to accelerate the end-to-end threat detection, investigation and response cycle.

[Learn more about QRadar.](#)

The post [Visibility and Threat Detection in a Remote Working World](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/posts/visibility-threat-detection-remote-work/>

9. Admin of carding portal behind \$568M in losses pleads guilty

Russian national Sergey Medvedev, one of the co-founders of Internet-based cybercriminal enterprise Infracard Organization and an admin on the organization's carding portal, today pleaded guilty to RICO conspiracy.

In February 2018, US authorities indicted 36 individuals for alleged roles in the transnational Infracard cybercrime group, out of 10,901 registered members in March 2017, and apprehended 13 defendants from the United States and six countries: Australia, the United Kingdom, France, Italy, Kosovo and Serbia.

"During the course of its seven-year history, the Infracard Organization inflicted approximately \$2.2 billion in intended losses, and more than \$568 million in actual losses, on a wide swath of financial institutions, merchants, and private individuals, and would have continued to do so for the foreseeable future if left unchecked," a DOJ release says.

Underground forum for selling financial info, PII, more

Infracard facilitated the large-scale acquisition, sale, and distribution of stolen identity information and payment cards, personally identifiable data, financial and banking info, computer malware, and various other contraband.

The Infracard organization also "directed traffic and potential purchasers to the automated vending sites of its members, which served as online conduits to traffic in

stolen means of identification, stolen financial and banking information, malware, and other illicit goods."

The operation and its website were active between October 2010 when it was created by Svyatoslav Bondarenko (at infraud[.]cc and infraud[.]ws, later moved to other locations) and until February 2018 when Infraud and its site were taken down following a joint operation between law enforcement agencies from seven countries.



Infraud takedown notice (DoJ)

All members needed admin approval to join

Infraud's forum hierarchy included administrators (4DMini57r470rz), super-moderators (Super MODER470R5), and moderators (M0d3r470r2) who oversaw the activity of users known as vendors (Doctors or Professors), VIP members (Fratello Masons or Advanced Members), and regular members (Phr4Ud573r).

To join Infraud's online forum, all users needed approval from one of the Infraud administrators and they also faced removal if the products they sold on the forum were considered subpar by the admins.

Medvedev, as one of Infraud's co-founder, operated an 'escrow' / currency exchanging service that ensured the transaction integrity between organization members. Medvedev

took the role of owner and admin of the Infraud Organization after Bondarenko went missing in 2015.

The roles of each of the defendants indicted two years ago are explained in detail in this second superseding criminal indictment filed on February 7, 2018.



Infraud hierarchy (DoJ)

Today, another Russian national, Aleksey Yurievich Burkov, was sentenced to 9 years in prison for operating Cardplanet and Direct Connection, two sites that facilitated payment card fraud, computer hacking, and other cybercrimes according to another release published today by DoJ officials.

The Cardplanet site was a card shop (also known as a CVV shop and carding site) where Burkov oversaw the selling of payment card (debit and credit card) numbers stolen from

hundreds of thousands of individuals, many of them U.S. Citizens, between at least early 2009 through at least August 2013.

The carding shop was also used to sell data from over 150,000 stolen payment cards which resulted in estimated fraud losses and fraudulent purchases of over \$20,000,000.

Source: <https://www.bleepingcomputer.com/news/security/admin-of-carding-portal-behind-568m-in-losses-pleads-guilty/>

10. COVID-19 ‘Breach Bubble’ Waiting to Pop?

The COVID-19 pandemic has made it harder for banks to trace the source of payment card data stolen from smaller, hacked online merchants. On the plus side, months of quarantine have massively decreased demand for account information that thieves buy and use to create physical counterfeit credit cards. But fraud experts say recent developments suggest both trends are about to change — and likely for the worse.

The economic laws of supply and demand hold just as true in the business world as they do in the cybercrime space. Global lockdowns from COVID-19 have resulted in far fewer fraudsters willing or able to visit retail stores to use their counterfeit cards, and the decreased demand has severely depressed prices in the underground for purloined card data.



An ad for a site selling stolen payment card data, circa March 2020.

That’s according to [Gemini Advisory](#), a New York-based cyber intelligence firm that closely tracks the inventories of dark web stores trafficking in stolen payment card data.

Stas Alforov, Gemini’s director of research and development, said that since the beginning of 2020 the company has seen a steep drop in demand for compromised “card present” data — digits stolen from hacked brick-and-mortar merchants with the help of malicious software surreptitiously installed on point-of-sale (POS) devices.

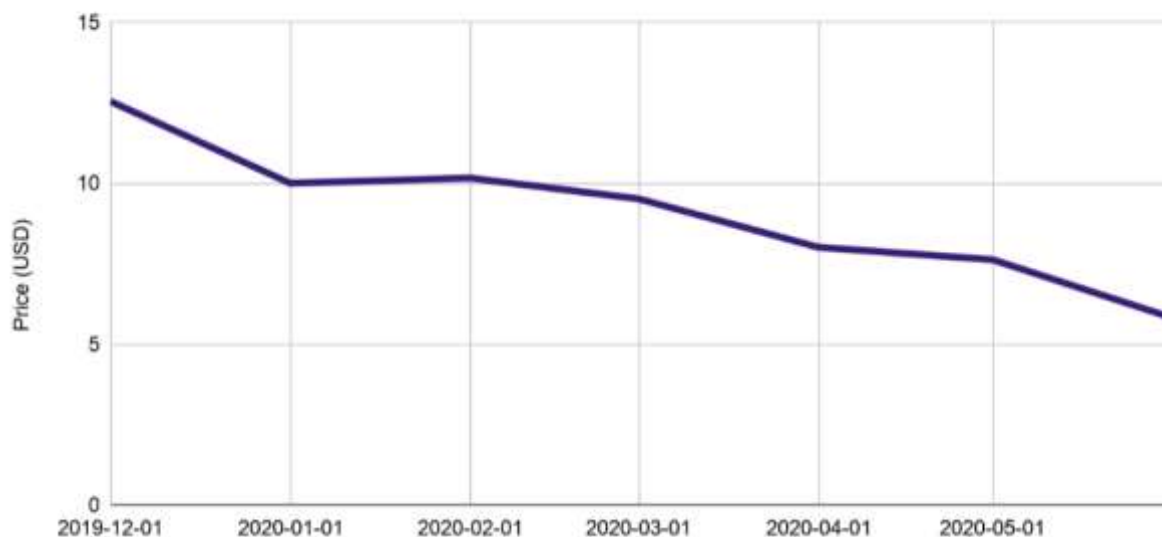
Alforov said the median price for card-present data has dropped precipitously over the past few months.

“Gemini Advisory has seen over 50 percent decrease in demand for compromised card present data since the mandated COVID-19 quarantines in the United States as well as the majority of the world,” he told KrebsOnSecurity.

Meanwhile, the supply of card-present data has remained relatively steady. Gemini’s [latest find](#) — a 10-month-long card breach at dozens of [Chicken Express](#) locations throughout Texas and other southern states that the fast-food chain first publicly acknowledged today after being contacted by this author — saw an estimated 165,000 cards stolen from eatery locations recently go on sale at one of the dark web’s largest cybercrime bazaars.

“Card present data supply hasn’t wavered much during the COVID-19 period,” Alforov said. “This is likely due to the fact that most of the sold data is still coming from breaches that occurred in 2019 and early 2020.”

MEDIAN PRICE PAID FOR COMPROMISED CARD PRESENT DATA



A lack of demand for and steady supply of stolen card-present data in the underground has severely depressed prices since the beginning of the COVID-19 pandemic. Image: Gemini Advisory

Naturally, crooks who ply their trade in credit card thievery also have been working from home more throughout the COVID-19 pandemic. That means demand for stolen “card-not-present” data — customer payment information extracted from hacked online merchants and typically used to defraud other e-commerce vendors — remains high. And so have prices for card-not-present data: Gemini found prices for this commodity actually increased slightly over the past few months.

Andrew Barratt is an investigator with [Coalfire](#), the cyber forensics firm hired by Chicken Express to remediate the breach and help the company improve security going forward. Barratt said there’s another curious COVID-19 dynamic going on with e-commerce fraud recently that is making it more difficult for banks and card issuers to

trace patterns in stolen card-not-present data back to hacked web merchants — particularly smaller e-commerce shops.

“One of the concerns that has been expressed to me is that we’re getting [fewer] overlapping hotspots,” Barratt said. “For a lot of the smaller, more frequently compromised merchants there has been a large drop off in transactions. Whilst big e-commerce has generally done okay during the COVID-19 pandemic, a number of more modest sized or specialty online retailers have not had the same access to their supply chain and so have had to close or drastically reduce the lines they’re selling.”

Banks routinely take groups of customer cards that have experienced fraudulent activity and try to see if some or all of them were used at the same merchant during a similar timeframe, a basic anti-fraud process known as “common point of purchase” or CPP analysis. But ironically, this analysis can become more challenging when there are fewer overall transactions going through a compromised merchant’s site, Barratt said.

“With a smaller transactional footprint means less Common Point of Purchase alerts and less data to work on to trigger a forensic investigation or fraud alert,” Barratt said. “It does also mean less fraud right now – which is a positive. But one of the big concerns that has been raised to us as investigators — literally asking if we have capacity for what’s coming — has been that merchants are getting compromised by ‘lie in wait’ type intruders.”

Barratt says there’s a suspicion that hackers may have established beachheads [breachheads?] in a number of these smaller online merchants and are simply biding their time. If and when transaction volumes for these merchants do pick up, the concern is then hackers may be in a better position to mix the sale of cards stolen from many hacked merchants and further confound CPP analysis efforts.

“These intruders may have a beachhead in a number of small and/or middle market e-commerce entities and they’re just waiting for the transaction volumes to go back up again and they’ve suddenly got the capability to have skimmers capturing lots of card data in the event of a sudden uptick in consumer spending,” he said. “They’d also have a diverse portfolio of compromise so could possibly even evade common point of purchase detection for a while too. Couple all of that with major shopping cart platforms going out of support ([like Magento 1 this month](#)) and furloughed IT and security staff, and there’s a potentially large COVID-19 breach bubble waiting to pop.”

With a majority of payment cards issued in the United States now equipped with a chip that makes the cards difficult and expensive for thieves to clone, cybercriminals have continued to focus on hacking smaller merchants that have not yet installed chip card readers and are still swiping the cards’ magnetic stripe at the register.

Barratt said his company has tied the source of the breach to malware known as “[PwnPOS](#),” an ancient strain of point-of-sale malware that first surfaced more than seven years ago, if not earlier.

Chicken Express CEO **Ricky Stuart** told KrebsOnSecurity that apart from “a handful” of locations his family owns directly, most of his 250 stores are franchisees that decide on their own how to secure their payment operations. Nevertheless, the company is now forced to examine each store’s POS systems to remediate the breach.

Stuart blamed the major point-of-sale vendors for taking their time in supporting and validating chip-capable payment systems. But when asked how many of the company’s 250 stores had chip-capable readers installed, Stuart said he didn’t know. Ditto for the handful of stores he owns directly.

“I don’t know how many,” he said. “I would think it would be a majority. If not, I know they’re coming.”

Source: <https://krebsonsecurity.com/2020/06/covid-19-breach-bubble-waiting-to-pop/>

11. Business giant Xerox allegedly suffers Maze Ransomware attack

Maze ransomware operators have updated their list of victims adding Xerox Corporation to the roster. It appears that the encryption routine had completed on June 25.

The company has yet to confirm or deny a cyberattack on its network but screenshots from the attacker show that computers on at least one Xerox domain have been encrypted.

Xerox Corporation is a huge business present in at least 160 countries. It registered over \$1.8 billion in revenue in Q1 2020 and has 27,000 employees across the globe. It's part of the Fortune 500 list, currently ranking at 347, with a revenue of over \$9 billion last year.

Threat to publish over 100GB of data

On June 24, for a brief while, Maze's leak site showed Xerox among the victims of this ransomware group. We contacted Xerox at the time but did not receive an answer.

The attackers told BleepingComputer that they had compromised the company’s network but added them too early.

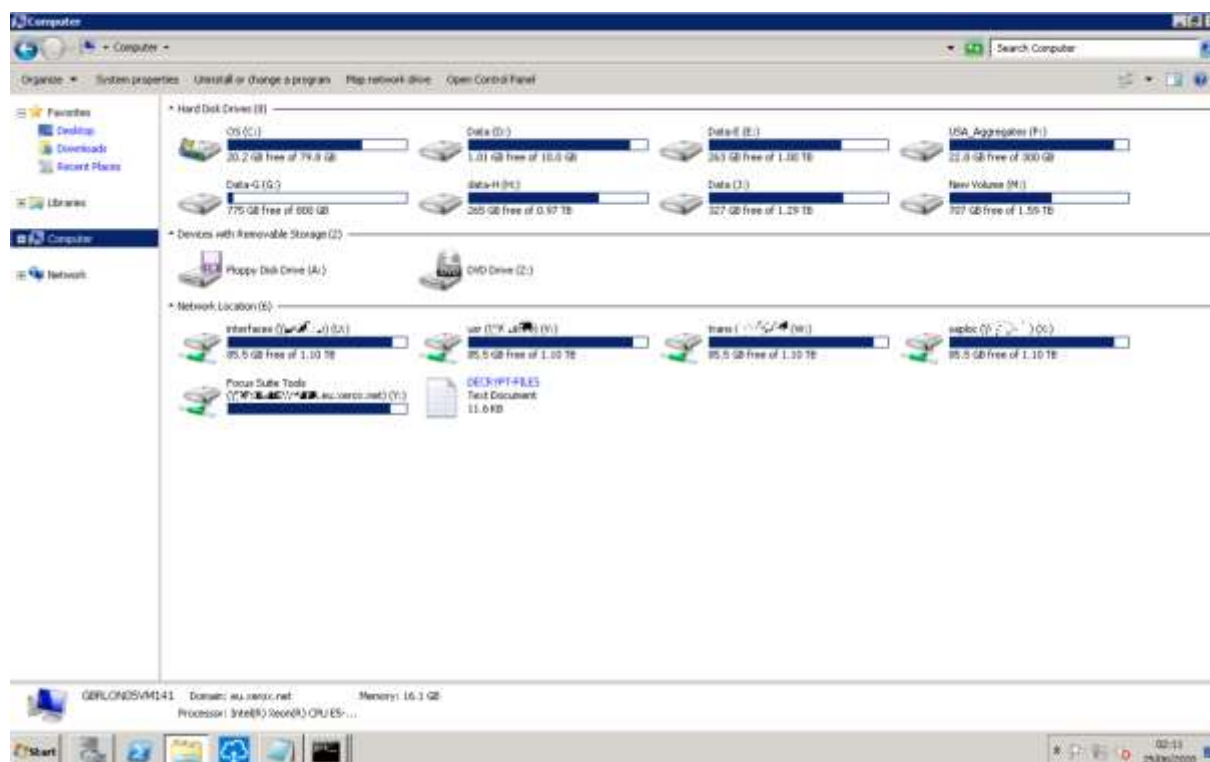
Just like previous posts from Maze, the one for Xerox lacks any details about the attack except for proof of the breach and of encrypting the company’s systems.

According to the attacker, they have stolen more than 100GB of files from Xerox and are determined to share it all if the company chooses not to engage in negotiations for a ransom payment.

“After the payment the data will be removed from our disks and decryptor will be given to you, so you can restore all your files,” reads the ransom note.

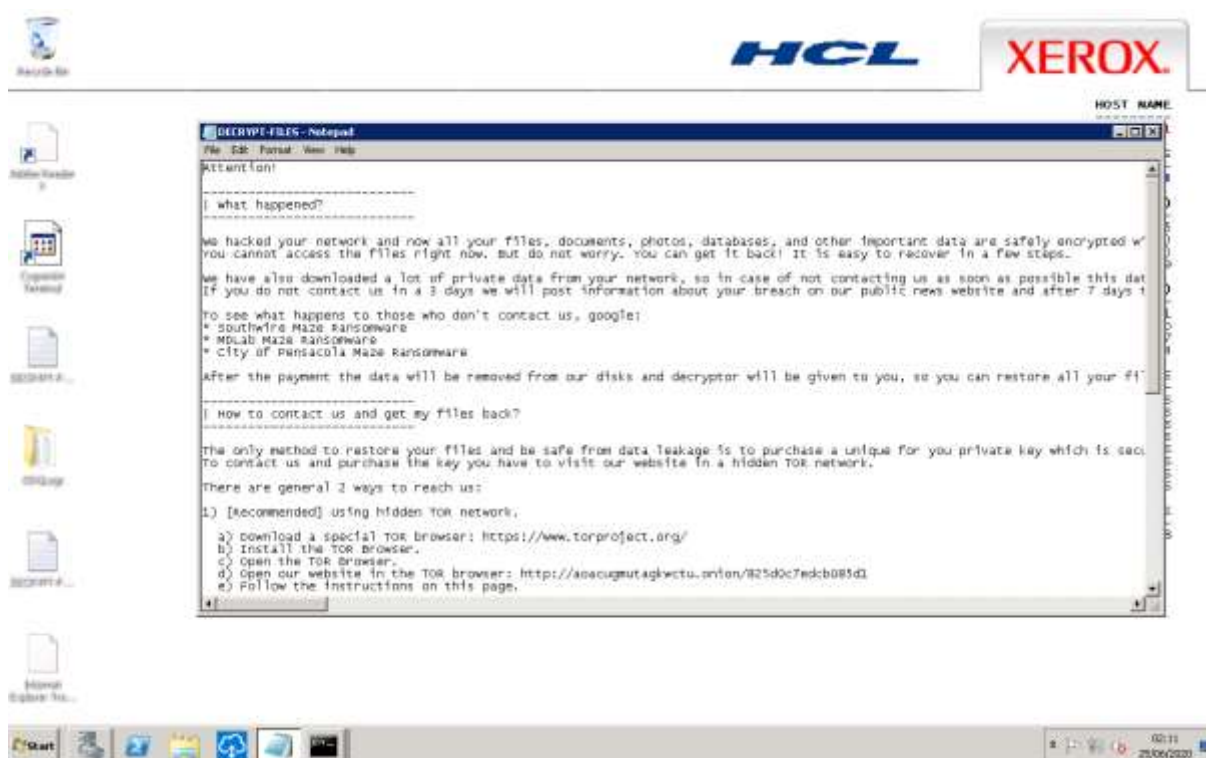
Maze published a set of 10 screenshots, showing directory listings from June 24 and 25, network shares, and the ransom note that is dropped after the encryption routine completes.

Specifically, one image shows that hosts on “eu.xerox.net,” managed by Xerox Corporation, were compromised. Systems on other domains might also be impacted.



While the domain reveals that Maze ransomware breached a Xerox branch in Europe, the names of the hosts hint that it's the one in London.

Another screenshot of a desktop screen with the Xerox brand name shows the ransom note dropped by the attacker, who threatened to publish information from the breach if the company did not contact them in three days.



Maze ransomware affiliates have been breaching big companies left and right. Some of the more recent attacks claimed by this group include LG Electronics, chip maker MaxLinear, IT giant Cognizant, and business services company Conduent.

Ransomware infections typically leverage exposed remote desktop services and then gain access to domain admin accounts. From there, they can pivot to valuable hosts. Vulnerabilities in systems that face the public web are also an entry point for these attackers.

Starting last year, ransomware groups began to steal data from the victim network and threaten to publish it unless the ransom is paid.

Source: <https://www.bleepingcomputer.com/news/security/business-giant-xerox-allegedly-suffers-maze-ransomware-attack/>

12. UCSF Pays \$1.14M After NetWalker Ransomware Attack

UCSF has paid more than \$1 million after a ransomware attack encrypted data related to “important” academic research on several servers.

The University of California, San Francisco (UCSF) has paid a \$1.14 million ransom to recover data related to “important” academic work. The data was encrypted after the NetWalker ransomware reportedly hit the UCSF medical school.

The UCSF, which includes a medical school and a medical center (UCSF Medical Center) as well as a graduate division, is a leading institution in biological and medical research. The university said that it first detected a “security incident” in its medical school’s IT environment on June 1. The attackers launched malware that encrypted a “limited number” of servers within the medical school, making them inaccessible.

“The data that was encrypted is important to some of the academic work we pursue as a university serving the public good,” said the university in a recent security update. “We therefore made the difficult decision to pay some portion of the ransom, approximately \$1.14 million, to the individuals behind the malware attack in exchange for a tool to unlock the encrypted data and the return of the data they obtained.”

Threatpost reached out to UCSF for more information about how the cyberattack started and whether they have received a decryption key that works.

The cyberattack did not affect the university’s patient care delivery operations, overall campus network, or COVID-19 work, it said. UCSF also said they “do not currently believe” patient medical records were exposed – but are continuing their investigation.

“Our investigation is ongoing but, at this time, we believe that the malware encrypted our servers opportunistically, with no particular area being targeted,” according to UCSF. “The attackers obtained some data as proof of their action, to use in their demand for a ransom payment.”

NetWalker Ransomware

According to a BBC report, the NetWalker ransomware is behind the attack. This ransomware family, which was behind a cyberattack on the Toll Group, recently transitioned to a ransomware-as-a-service (RaaS) model, and its operators are placing a heavy emphasis on targeting and attracting technically advanced affiliates.

The healthcare sector has been a prime target for the ransomware group, particularly during the ongoing pandemic. The group was reportedly behind a ransomware attack

on the website of Champaign-Urbana Public Health District in Illinois earlier in 2020, for instance.

During the cyberattack on UCSF, the operators reportedly sent the university an initial ransom demand of \$3 million, noting that the university made billions a year, according to BBC's report. After back-and-forth negotiations, the ransomware operator made a final offer of \$1.14. Since then, UCSF has transferred 116.4 Bitcoins to the attacker's electronic wallet, and has since received decryption software.

After detecting the attack, UCSF isolated the affected IT system in the medical school's environment so that the core UCSF network was not affected. The university also has been working with a leading cyber-security consultant and other outside experts to investigate the incident, and said it expects to fully restore the affected servers soon.

Paying The Ransom

The act of paying the ransom after a ransomware attack has long drawn criticism by security experts, who say that the payouts fund future malicious activities by cybercriminals, and gives them more incentive to launch further attacks. Experts say, paying the ransom also can inspire other cybercriminals to launch similar attacks in hopes of making money. Some states, like New York, have even considered potentially banning municipalities from paying ransomware demands.

Brett Callow, threat analyst with Emsisoft, told Threatpost that paying the ransom leads to a "vicious circle" and the only way to break it is for companies to stop paying.

"Some consider the question of whether to pay ransoms to be purely business decisions that companies should make on the basis of simple cost-benefit analyses. This, of course, is a very shortsighted view," Callow said. "Paying ransoms further incentivizes the criminals and provides them with additional resources to invest in scaling up their operations. That means more victims, and more ransoms paid."

Ransom payouts can also be a costlier approach for ransomware victims. Recent research conducted by Vanson Bourne and commissioned by security firm Sophos showed that ransomware victims that refused to pay a ransom reported, on average, \$730,000 in recovery costs – while organizations that did pay a ransom reported an average total cost, including the ransom, of \$1.4 million.

Despite these warnings, it's not uncommon for ransomware victims to pay up. Travelex this year paid out \$2.3 million to hackers to regain access to its global network after a January malware attack knocked the global currency exchange offline and crippled its business. And in 2019, a Florida city, hit by a ransomware attack that crippled its

computer systems for three weeks, paid the attackers the requested ransom of \$600,000.

Source: <https://threatpost.com/ucsf-pays-1-14m-after-netwalker-ransomware-attack/157015/>

13. New Phishing scam targets website owners with free DNSSEC offer

A very clever phishing campaign targets bloggers and website owners with emails pretending to be from their hosting provider who wants to upgrade their domain to use secure DNS (DNSSEC).

As it's possible to determine who is hosting a domain for a website via the WHOIS records, IP addresses, and HTTP headers, the email scam is highly targeted and impersonates the specific hosting company used by a website.

In a new report by Sophos, researchers explain how the scammers are using this WHOIS information to send targeted emails that impersonate WordPress, NameCheap, HostGator, Microsoft Azure, and other well-known hosting companies.

The security company was first alerted to this scam when they received the phishing scam pretending to be WordPress, who hosts their NakedSecurity blog.



Phishing email sent to website owners

Source: Sophos

Domain Name System (DNS) is the technology that is analogous to a real-world "phone book." It maps and resolves the memorable domain names such as bleepingcomputer.com into the corresponding IP address of the server (in this case, 104.20.59.209), where the website is hosted.

There is a newer protocol, DNSSEC, that exists to provide extra security to DNS queries and responses. This feature is typically implemented as a safeguard by domain hosting providers to prevent DNS data from being tampered.

These phishing emails state that the website's DNS provider will be upgrading their DNS to secure DNS (DNSSEC), but need them to click on a link to activate this enhanced security feature.

Sophos' report explains that DNSSEC is not something website owners would typically setup on their own.

"You've probably never set up DNSSEC or used it directly yourself because it has typically been a feature used by service providers to help to keep their DNS databases intact when they exchange data with other DNS servers," the report explained.

Considering most independent bloggers and webmasters would seldom have a reason to look into DNSSEC, the spammers exploit their curiosity and fear through this campaign.

Once the malicious links in the email are clicked, a "surprisingly believable" Update Assistant page is generated on the fly.



Fake WordPress Update Assistant landing page

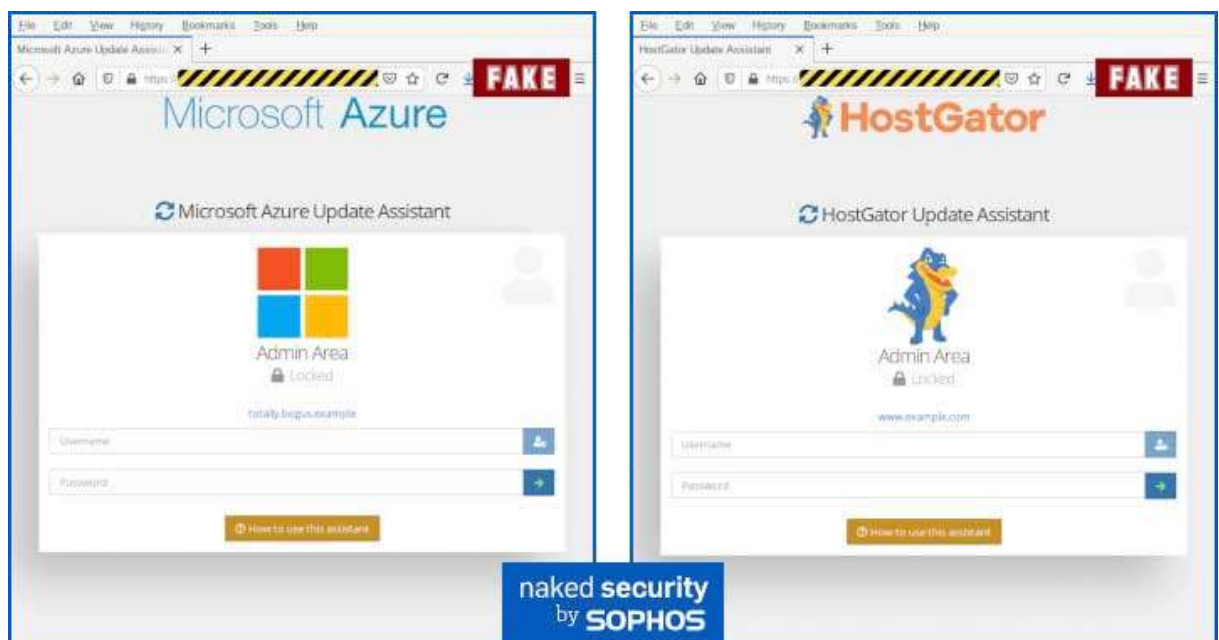
Source: Sophos

Of interest, is that these pages are dynamically generated based on the base64-encoded GET parameters in the URL. These parameters instruct the backend to render the page with the appropriate website name, logo, and the URL of the client website.

For example, the link within the phishing email Sophos team received, had the base64 encoded "banner" parameter set to WordPress, which is their hosting provider, and the "URL" set to base64-equivalent of "nakedsecurity.sophos.com"

[https://\[REDACTED\].com/?banner=V29yZFB5ZXNz&url=bmFrZWZrZWN1cmI0eS5zb3Bo b3MuY29t](https://[REDACTED].com/?banner=V29yZFB5ZXNz&url=bmFrZWZrZWN1cmI0eS5zb3Bo b3MuY29t)

The Sophos team further demonstrated how they could simply alter these two parameters, and new pages would be generated on the fly to impersonate different hosting providers.



Modifying URL parameters to generate different scams

As the attackers forgot to turn off directory indexing on their malicious phishing domain, Sophos could see all the logos of different hosting providers they had hosted on their server.

```
[. . . . .]
[IMG] HostGator.png                25-Jun-2020 19:04    12k
[IMG] HostGator_avatar.png         25-Jun-2020 19:06    12k
[IMG] HostMonster.png              25-Jun-2020 20:15    12k
[IMG] HostMonster_avatar.png       25-Jun-2020 20:17     4k
[IMG] KonaKart.png                  26-Jun-2020 01:50    16k
[IMG] KonaKart_avatar.png           26-Jun-2020 01:50     8k
[IMG] Linode.png                    25-Jun-2020 19:07    12k
[IMG] Linode_avatar.png             25-Jun-2020 19:09     8k
[IMG] Magento.png                   22-Nov-2018 19:29    12k
[IMG] Magento_avatar.png            22-Nov-2018 19:32     8k
[IMG] Microsoft Azure.png           25-Jun-2020 20:10    12k
[IMG] Microsoft Azure_avatar.png    25-Jun-2020 20:11     4k
[IMG] Name Cheap.png                25-Jun-2020 20:22    16k
[IMG] Name Cheap_avatar.png         25-Jun-2020 20:23     8k
[IMG] Network Solutions.png         25-Jun-2020 19:15    12k
[. . . . .]
```

Impersonated hosting companies

Some prominent names of hosting companies impersonated include HostGator, HostMonster, KonaKart, Linode, Magento, Microsoft Azure, NameCheap, and Network Solutions.

The goal of this phishing campaign is to steal credentials from unsuspecting users rather than offering them any legitimate DNSSEC protection service.

Once the user enters their credentials, the malicious website pretends to kick off a series of installation and “update” sequences, using bogus AJAX-style loaders and popup alerts, imitating an installation.

Users are told that once the update completes, they will be redirected to their website. But this doesn’t happen, perhaps due to a programming error on the scammers’ part.

“As you can see, the crooks claim that you’ll be redirected to your own site at the end of the process, but instead you end up at a URL that includes the name of your site preceded by the name of the fake site set up by the crooks. This produces a 404 error – what we can’t tell you is whether the crooks made a programming blunder and accidentally redirected you to https://[THEIRDOMAIN]/your.example instead of directly to https://your.example or whether they intended this all along, to avoid redirecting to you directly to your own login page, which might seem suspicious given that you put in your username and password already,” Sophos states in their report.

As a general rule, to safeguard against scams like these, email recipients should be mindful of the links they click in an email and especially when entering their credentials on unfamiliar sites and systems.

Enabling two-factor authentication can also help deter phishing attacks that attempt to steal login credentials.

Source: <https://www.bleepingcomputer.com/news/security/new-phishing-scam-targets-website-owners-with-free-dnssec-offer/>

14. The Modern Workplace: Keeping Remote Workers Productive and Secure

Results from the March 30, 2020, [Gartner CFO Survey](#) indicate that 74% of businesses intend to shift some employees to permanent remote work following their initial experience responding to current global conditions.

Regardless of recent world events, many workers already spend time on the job, while physically separated from the corporate campus. Sometimes they will use a work-provided computer, while other times they may opt for a personal device for convenience. In either scenario, it is imperative that businesses ensure remote workers are enabled with access to the tools they need to be productive, while keeping workers and corporate information safe.

Key Challenges to Enabling Remote Work

Businesses are having to enable remote-work capabilities faster than ever, yet their traditional security methods aren't built to support this use case. Forcing remote work into a traditional, perimeter-based security model results in performance issues, a reduction in productivity and a poor overall user experience.

There are a number of challenges that companies will need to overcome to ensure that employees are enabled to work remotely, while remaining secure and productive:

- Identifying authorized users.
- Managing devices and publishing best practices for a diverse workforce.
- Ensuring devices, managed or not, comply with the needed security standards.
- Operationalizing remote security monitoring.

A new, cloud-delivered approach is needed to support the real-world use cases of working remotely.

Managing and Securing Access to Applications

Companies of all sizes have been grappling with secure access management in increasingly cloud- and mobile-first environments for several years. Aside from a few legacy services, the majority of heavily-trafficked enterprise applications are software-as-a-service (SaaS) based, sitting outside of the organization's perimeter. For many organizations, identity has had to become the new perimeter, because the traditional perimeter has become increasingly ineffective in providing robust, consistent security for their application infrastructures.

Establishing a user's identity is key to managing security within a remote working setup. The use of multifactor authentication (MFA) and single sign-on (SSO) provides a high level of assurance to a session that isn't granted with basic usernames and passwords.

Identity alone is not enough. The device also needs to be assessed. A user's identity should not vouch for the health of the device they are using; they may have unwittingly installed malware or their operating system (OS) may not be patched. Companies need to start moving to a contextual security model that is able to assess multiple data points to determine the risk associated with an access request.

The need for Zero Trust access security becomes clear, particularly in light of today's crisis. Many security professionals are now pushing for access control policies that can incorporate some information about the device, its risk state, the location from which the request is initiated and other salient details on the user and application before a request can be granted. A user's identity then determines what they should have access to, obscuring services irrelevant to their level. This is a big change from the checks in place with legacy solutions, but a significant step forward to improve the organization's security posture.

Managing Devices Used by Remote Workers

Part of business continuity is about maintenance and ensuring that existing technologies are patched and up to date. [Unified Endpoint Management \(UEM\)](#) tools will play an important role in how remote workers are managed over the coming months, enabling information technology (IT) teams to enroll new devices, including bring your own device (BYOD), as well as configure devices so they comply with corporate policy. This can be anything from installing VPN profiles, enforcing encryption or provisioning new content and services.

Enforce Acceptable Usage Policies

In today's modern workplace, employees can access any site, anywhere at any time. This can also mean the wrong sites in the wrong places and at the wrong times. If left unmanaged, such services as Netflix, YouTube and Spotify, can tear through your data allowance and rack up costs. Organizations need to ensure personalized usage is capped or blocked based on what is considered "acceptable usage." This can help preserve productivity and security and ensure compliance with the growing number of regulations that affect data management.

Organizations need to invest in good documentation so employees know how to get online and how to access and use approved tools. [Acceptable use policies](#) need to be documented, as well as approved devices and apps. This will help reduce help desk strain by proactively distributing instructions that detail how employees should connect remotely.

Although maintaining policies is important, having employees read and follow all instructions can be difficult. In addition to having written guidelines on what usage is not acceptable, businesses should also manage policies from the cloud that only allow the correct tools to be used or appropriate browsing to occur. Building intelligence into these policies allows them to be dynamic and change based on the context. When there are changes, they are applied instantly from the cloud rather than waiting for apps to update or employees to read documentation. This approach means end users and administrators don't need to worry about regulations and compliance; it is taken care of by the acceptable use policy that is applied automatically.

Protect Remote Workers and the Data They Need

Uncertainty is a cybercriminal's best friend, and this current state of global uncertainty presents the perfect opportunity. We've already seen a number of phishing and malware attacks using this particular moment's headlines as a guise. As millions of people look to make sense of the situation, it's very easy for them to be lured in by scams pretending to provide new information, answers or even potential remedies.

With conflicting misinformation available, people are stressed, vulnerable and afraid. Awareness training alone will not suffice in these circumstances; cyber protection for workers needs to be upped. Many of these threats are new, taking advantage of social media and other vectors for rapid dissemination. Unless security products are able to respond rapidly to a sudden change in tactics and protect against zero-day attacks, then this could prove a gaping hole in security.

Additionally, the number of devices connecting to corporate services will likely continue to be on the rise. If companies don't already have a BYOD policy in place, they may be forced to adopt one due to a lack of inventory or capability for employees to work

remotely. Personal devices may not live up to the security standards required by companies. Systems may need updating, malicious applications may be installed or credentials may have been phished. Operating beyond the corporate perimeter means companies need a security solution fit to operate in a less predictable environment.

Operationalizing Security for the Distributed Organization

The number of tools administrators need to monitor and operate business security and regulatory compliance has expanded in recent years. An IDC survey reported that more than half of businesses use more than 10 network and application components to add a new external user group to an organization. Managing policies and threat hunting can be similarly difficult as teams navigate through multiple tools.

For security solutions to be effective and efficient, they need to work together to form an integrated ecosystem. Utilizing existing enterprise directory systems is a simple way that policy coordination can be managed. Syncing existing enterprise directory systems is a simple way that policy coordination can be achieved, as any user groups or individuals change, policy configurations in each security tool are updated automatically. Stream logs from different security services into a centralized SIEM or SOAR provide administrators with condensed visibility, enabling end-to-end threat hunting.

The Future of Remote Working

Nearly every company is being forced to address remote-working inefficiencies and insecurities that have been perceived as minor niggles for the past decade. With mass adoption of remote-working practices, they can no longer be tolerated, as the new age of working is here, probably to stay. In these circumstances, technology can be friend or foe. Companies that can adapt the quickest, and provision technologies that keep employees the most productive and secure will have the best chance of survival.

The post [The Modern Workplace: Keeping Remote Workers Productive and Secure](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/posts/keeping-remote-workers-data-secure/>

15. Microsoft releases urgent security updates for Windows 10 Codecs bugs

Microsoft has released two out-of-band security updates to address remote code execution security vulnerabilities affecting the Microsoft Windows Codecs Library on several Windows 10 and Windows Server versions.

The two vulnerabilities are tracked as CVE-2020-1425 and CVE-2020-1457, the first one being rated as critical while the second received an important severity rating.

Both desktop and server platforms affected

In both cases, the remote code execution issue is caused by the way that Microsoft Windows Codecs Library handles objects in memory.

After successfully exploiting CVE-2020-1425, attackers "could obtain information to further compromise the user's system," while successful exploitation of CVE-2020-1457 could lead to arbitrary code execution on vulnerable systems.

Exploitation of these vulnerabilities requires a program to process a specially crafted image file.

According to Microsoft, the two out-of-band security updates address the vulnerabilities "by correcting how Microsoft Windows Codecs Library handles objects in memory."

Affected systems include Windows 10 versions 1709 or later desktop platforms and Windows Server 2019 and several Windows Server (Server Core installation) versions for both security issues.

No mitigation available, updates will install automatically

Microsoft says that it has not identified any mitigating measures or workarounds for these two vulnerabilities.

"Affected customers will be automatically updated by Microsoft Store. Customers do not need to take any action to receive the update," Microsoft explains,

"Alternatively, customers who want to receive the update immediately can check for updates with the Microsoft Store App; more information on this process can be found [here](#)."

Both vulnerabilities were reported to Microsoft by vulnerability analysis manager Abdul-Aziz Hariri through Trend Micro's Zero Day Initiative.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-releases-oob-security-updates-for-windows-10-rce-bugs/>

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

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.