

# Monthly Security Bulletin

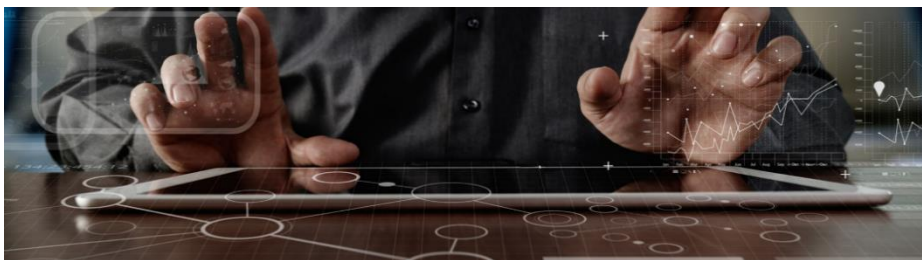


# This security bulletin is powered by Telelink's Advanced Security Operations Center

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!**

**TELELINK PUBLIC**

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

## What is inside:

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

## Table of Contents

|     |  |    |
|-----|--|----|
| 1.  | Cybersecurity Gaps and Opportunities in the Logistics Industry .....         | 4  |
| 2.  | European Banking Authority discloses Exchange server hack.....               | 6  |
| 3.  | Why the Demand for Application Development Security Skills Is Exploding..... | 7  |
| 4.  | z0Miner botnet hunts for unpatched ElasticSearch, Jenkins servers.....       | 10 |
| 5.  | Chinese state hackers target Linux systems with new malware .....            | 11 |
| 6.  | Why MITRE ATT&CK Matters? .....  | 13 |
| 7.  | Phishing sites now detect virtual machines to bypass detection .....         | 16 |
| 8.  | The Week in Ransomware - March 19th 2021 - Highest ransom ever! .....        | 18 |
| 9.  | Microsoft warns of phishing attacks bypassing email gateways .....           | 21 |
| 10. | Microsoft improves Windows Sandbox in latest Windows 10 build .....          | 22 |
| 11. | Engineer reports data leak to nonprofit, hears from the police.....          | 26 |
| 12. | FBI exposes weakness in Mamba ransomware, DiskCryptor .....                  | 29 |
| 13. | Ransomware admin is refunding victims their ransom payments .....            | 31 |
| 14. | Microsoft Exchange attacks increase while WannaCry gets a restart.....       | 33 |
| 15. | Malicious Docker Cryptomining Images Rack Up 20M Downloads.....              | 36 |

# 1. Cybersecurity Gaps and Opportunities in the Logistics Industry

Shipping and logistics is, in many ways, the backbone of our lives and businesses. What business doesn't benefit from fresh food or a timely delivery? Unfortunately, this industry is open to cyberattacks just like anyone else. Luckily, groups in the trucking and logistics industry aren't powerless to address these challenges. Check out how you can begin to take a strategic approach to security on the road.

## Recent Cyberattacks on the Logistics Sector

Trucking and logistics companies suffered their fair share of cyber attacks in 2020. In October 2020, a U.S. flatbed trucking group said ransomware had affected one of its operating companies. They made this announcement after the [Conti ransomware group](#) posted files from what it claimed was the operating company to the dark web.

A trucking and freight transportation logistics company suffered a Hades malware infection in December 2020. In response, the company was forced to [take all of its IT systems offline](#) while it dealt with the attack.

The [COVID-19 vaccine supply chain](#) has also been attacked, this time using the venerable method of phishing emails. A threat actor broke into a German biomedical company critical to the COVID-19 cold chain. From there, they launched phishing emails to its partners involved with transporting the vaccine.

So, what's going on in the trucking and logistics industry that's fueling these attacks?

## Cybersecurity Challenges Abound

Trucking and logistics groups are grappling with several digital challenges at once. One of the most important of those is balancing defense with modern tools. Most businesses in this sector use sensors and other [Internet of things](#) (IoT) devices to help them monitor and manage their [supply chain](#) operations.

On the one hand, these tools yield useful connections. On the other, they complicate things by adding smart products into the network that often lack security by design. Malicious actors could abuse software flaws within those devices to disrupt business.

The supply chain itself is also at risk. Like businesses in other industries, many logistics and trucking entities grant network access to their vendors, partners and suppliers. This decision promotes connectivity and efficiency, thereby helping these groups keep their schedules. But, it also expands the attack surface. This access makes it possible for a malicious actor to compromise one of those third parties. From there, they can misuse their network access to breach their trucking and logistics partner.

## The Human Element

Lastly, many trucking and logistics entities lack the know-how to defend themselves against these types of digital threats. In a 2019 report, for instance, [Eye for Transport](#) (EFT) found that fewer than half (43%) of trucking and logistics organizations had a chief information security officer (CISO). That didn't bother most respondents, however, only 21% of them told EFT they felt they needed a CISO's expertise.

These findings underscore two problems. First, not having a CISO means a company [probably](#) doesn't have a formal plan in place for addressing threats either. Second, in the view that they don't need a CISO, most entities implicitly ignore the importance of a good defense. If you don't believe you need expert guidance in the first place, you won't get an expert to deal with it. But not taking any meaningful approach to their defense isn't a solution. It leaves every window and door open to malicious actors.

## Best Practices for Cybersecurity in Logistics

Taking a strategic approach means researching vendors that take a serious approach to the security of their smart products. You'll know they're serious if they release firmware updates remotely and allow customers to change the default admin credentials. You should also consider using [network segmentation](#) to isolate IoT devices. Doing so will help to prevent a potential compromise of one of these smart products from spreading to the rest of the IT network.

Moving on to supply chain security, entities need to carefully choose their vendors and build an inventory of their selected partners. They can then use service-level agreements to require that vendors complete a risk assessment in order to maintain their business partnership. With those results in hand, trucking and logistics entities can remediate certain weaknesses by drawing on the strength of their connections with their vendors, suppliers and partners. This will enable them to implement data encryption and other security best practices as well as to formulate an [incident response plan](#) if and when a supply chain security incident occurs.

Finally, trucking and logistics organizations can accomplish all of these suggestions and more by working with a trusted [managed security services provider](#). Doing so will not only guide your cybersecurity program, but will also help to build a positive security culture within the workplace. You might not have a CISO, but with the right provider, you'll have the security expertise your business needs to adapt to the changing threat landscape and minimize digital security risk going forward.

Source: <https://securityintelligence.com/articles/cybersecurity-in-logistics-gaps-and-opportunities/>

## 2. European Banking Authority discloses Exchange server hack

The European Banking Authority (EBA) took down all email systems after their Microsoft Exchange Servers were hacked as part of the ongoing attacks targeting organizations worldwide.

EBA is part of the European System of Financial Supervision and it oversees the integrity orderly functioning of the EU banking sector.

"The Agency has swiftly launched a full investigation, in close cooperation with its ICT provider, a team of forensic experts and other relevant entities," EBA said.

"The EBA is working to identify what, if any, data was accessed. Where appropriate, the EBA will provide information on measures that data subjects might take to mitigate possible adverse effects."

An initial advisory published Sunday said that the attackers might have gained access to personal information stored on the email servers.

However, an update issued today added that forensic experts had found no signs of data exfiltration.

"The EBA investigation is still ongoing and we are deploying additional security measures and close monitoring in view of restoring the full functionality of the email servers," the EU agency said.

"At this stage, the EBA email infrastructure has been secured and our analyses suggest that no data extraction has been performed and we have no indication to think that the breach has gone beyond our email servers."

## Widespread attacks targeting organizations worldwide

Last week, Microsoft patched multiple zero-day vulnerabilities affecting on-premises versions of Microsoft Exchange Server and exploited in ongoing attacks coordinated by multiple state-sponsored hacking groups.

At first, Microsoft only linked the attacks to a China state-sponsored hacking group dubbed Hafnium.

In an update to the blog post, the company says several other threat actors exploit the recently patched Exchange flaws in similar campaigns.

While Hafnium's targets' identities are not yet known, Microsoft has shared a list of previously targeted industry sectors.

"Historically, Hafnium primarily targets entities in the United States for the purpose of exfiltrating information from a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs," Microsoft VP Tom Burt said.

The Chinese-backed APT27, Bronze Butler (aka Tick), and Calypso are also attacking unpatched Exchange servers, according to Slovak internet security firm ESET, who says that it also detected other state-sponsored groups it couldn't identify.

CISA also warned of "widespread domestic and international exploitation of Microsoft Exchange Server vulnerabilities" on Saturday, urging admins to use Microsoft's IOC detection tool to detect signs of compromise in their organizations.

The attackers deploy web shells that allow them to gain remote access to a compromised server and to the internal network, even after the servers are patched.

Microsoft has updated their Microsoft Safety Scanner (MSERT) tool to detect web shells deployed in these attacks and a PowerShell script to search for indicators of compromise (IOC) in Exchange and OWA log files.

*Source: <https://www.bleepingcomputer.com/news/security/european-banking-authority-discloses-exchange-server-hack/>*

### 3. Why the Demand for Application Development Security Skills Is Exploding

Application development security is a key task when it comes to looking to the future of cybersecurity. A [recent industry study](#) shows it is the fastest-growing cybersecurity skill for the year ahead. Demand is expected to increase by 164% over the next five years. Such growth would bump up the total number of job openings requiring this skill from 29,635 in 2020 to 48,601 a few years from now.

These findings raise important questions. What is application development security? And, what's driving the rapid growth?

#### Application Development Security at a Glance

First, this job is about strengthening the defenses of an app by finding and fixing openings. As the name implies, this process most often takes place within the



development phase before an app goes into production. But it can occur after the owner has deployed those apps, as well.

There's not just one approach to looking at application development security, otherwise known as application security testing (AST). The several methods people in this field will probably use include the following:

- **Static Application Security Testing (SAST):** In this type of web application security testing, the defense experts on the job have some knowledge about an application's architecture. They can use this knowledge to report weaknesses within the source code.
- **Dynamic Application Security Testing (DAST):** As opposed to SAST, DAST assumes no knowledge of an application's code. Its purpose is to find potential openings within a specific app's running state.
- **Interactive Application Security Testing (IAST):** This method combines SAST and DAST together into a hybrid approach.

## Why the Need for Application Development Security?

The growing demand for application development security reflects two ongoing trends.

1. The world is becoming more mobile. Businesses and other groups invest in their users being able to interact with their services via an app on a variety of devices. Along the way, they need someone with application development security skills to secure those apps in order to ensure consistent and secure mobile performance for a growing portion of their user base.

2. Openings in an app's defenses erode trust between the creators and the users. Overall, flaws like this are common in mobile apps. Almost three-quarters of iOS and Android apps analyzed [for a 2020 study](#) wouldn't have passed a basic security test. More than four-fifths (83%) of those surveyed apps had at least one flaw, with openings showing up in 91% of iOS apps and 95% of Android apps analyzed in the study.

## Keep Your Business Secure

Those holes pose a threat to businesses. Weak server-side controls, unsafe data storage, broken cryptography and other problems open the door for external attackers to [scrape information](#). Potential customers might hesitate to do business with groups that suffered a data breach because of poor application development security. That's assuming those groups can continue to operate after paying for repairs, paying the legal fees and other damages that come with a breach.

Lastly, some customers aren't even waiting that long to demand application development security matters. Customers are [telling companies](#) whose apps and other products they use to write more secure code before they've even faced an attack. In some cases, the

pressure supplied by customers dwarfed the pressure provided by regulators and compliance auditors. This shows how application development security is becoming a means by which organizations can maintain trusting partnerships with their customers from the moment they begin doing business together, not just in the aftermath of a publicly disclosed problem.

## Best Practices for Developers

Just as the defensive skills most needed by workplaces change, so do the skills themselves. Software composition analysis tools along with limited defense testing built right into developers' toolchains [could replace](#) older AST methods within the next few years. Industry experts predict that automated solutions will be capable of fixing 10% of openings spotted by SAST tools by 2022.

These forecasts provide a glimpse into where application development security as a field is going. But they don't detract from the basic practices that developers can use on their side to produce secure apps. For instance, developers need to realize there's rarely a need for them to write their own code from scratch. They don't have to hope they get defense right. Instead, they can use [secure frameworks](#) to power their code forward. They should also make sure they're using the latest versions of third-party code or libraries.

Developers should remember the power of teamwork, too. They can join forces with security architects and the operations team in order to implement [threat modeling](#). This process won't just help find and triage potential threats. It also fosters communication and mutual understanding — the foundations of [building a DevSecOps culture](#).

## Application Development Security for the Future

Like we said at the top, application development security is the way for organizations to ensure their place in the future. The tools and methods for putting application security in place might change, but the basics of security will remain relevant throughout the next few years and beyond.

The post [Why the Demand for Application Development Security Skills Is Exploding](#) appeared first on [Security Intelligence](#).

Source: <https://securityintelligence.com/articles/why-demand-for-application-development-security-skills-exploding/>

## 4. z0Miner botnet hunts for unpatched ElasticSearch, Jenkins servers

A cryptomining botnet spotted last year is now targeting and attempting to take control of Jenkins and ElasticSearch servers to mine for Monero (XMR) cryptocurrency.

z0Miner is a cryptomining malware strain spotted in November by the Tencent Security Team, who saw it infecting thousands of servers by exploiting a Weblogic security vulnerability.

Now, the attackers have upgraded the malware to scan for and attempt to infect new devices by exploiting remote command execution (RCE) vulnerabilities impacting ElasticSearch and Jenkins servers.

### Probing for servers left unpatched for years

According to a report published by researchers at Qihoo 360's Network Security Research Lab (360 Netlab), z0Miner is now probing for servers unpatched against vulnerabilities addressed in 2015 and earlier.

The botnet uses exploits targeting an ElasticSearch RCE vulnerability tracked as CVE-2015-1427 and an older RCE impacting Jenkins servers.

After compromising a server, the malware will first download a malicious shell script, starts hunting for and killing previously deployed cryptominers.

Next, it sets up a new cron entry to periodically grab and execute malicious scripts from Pastebin.

The next stage of the infection flow involves downloading a mining kit containing an XMRig miner script, a config file, a starter script, and starting to mine cryptocurrency in the background.

360 Netlab found that one of the Monero wallets used by the z0Miner botnet contains roughly 22 XMR (just over \$4600).

However, even if this doesn't seem like much, cryptomining botnets regularly use more than one wallet to collect illegally earned cryptocurrency that can quickly add up.

According to honeypot stats shared by 360 Netlab, the z0Miner botnet activity has started picking up again during mid-January after a short break in early-January.

## Thousands of devices already compromised

z0Miner became active last year and was spotted by the Tencent Security Team while exploiting two Weblogic pre-auth RCE bugs tracked as CVE-2020-14882 and CVE-2020-14883 to spread to other devices.

According to Tencent Security Team estimations, the threat actor controlling z0Miner compromised and quickly took over 5,000 servers.

The attackers scanned cloud servers in batches to find unpatched Weblogic servers and compromised them by sending "carefully constructed data packets" to exploit the vulnerable devices.

After compromise, z0Miner used a similar attack logic as the one observed by 360 Netlab researchers, gaining persistence via crontab and starting to mine for Monero.

The z0Miner sample found by Tencent Security Team in November 2020 was also spreading laterally on the network of already compromised devices via SSH.

Source: <https://www.bleepingcomputer.com/news/security/z0miner-botnet-hunts-for-unpatched-elasticsearch-jenkins-servers/>

## 5. Chinese state hackers target Linux systems with new malware

Security researchers at Intezer have discovered a previously undocumented backdoor dubbed RedXOR, with links to a Chinese-sponsored hacking group and used in ongoing attacks targeting Linux systems.

The RedXOR malware samples found by Intezer were uploaded to VirusTotal (1, 2) from Taiwan and Indonesia (known targets for Chinese state hackers) and have low detection rates.

Based on command-and-control servers still being active, the Linux backdoor is being used in ongoing attacks targeting both Linux servers and endpoints.

RedXOR comes with a large set of capabilities, including executing commands with system privileges, managing files on infected Linux boxes, hiding its process using the Adore-ng open-source rootkit, proxying malicious traffic, remote updating, and more.



## Links to Chinese Winnti malware

The new malware is believed to be a new malicious tool added to China's Winnti umbrella threat group's arsenal.

"Based on victimology, as well as similar components and Tactics, Techniques, and Procedures (TTPs), we believe RedXOR was developed by high profile Chinese threat actors," Intezer said.

Intezer also found multiple connections between the RedXOR Linux backdoor and multiple malware strains linked to the Winnti state hackers, including the PWNLNK backdoor and the Groundhog and XOR.DDOS botnets.

Similarities discovered by the security researchers while comparing these malware strains include the use of:

- old open-source kernel rootkits,
- identically named functions,
- XOR-encoded malicious traffic,
- comparable naming scheme for persistence services,
- compilation using legacy Red Hat compilers,
- very similar code flow and functionality, and more.

## Who is Winnti?

Winnti is an umbrella term used to track a collective of state-backed hacking groups (BARIUM by Microsoft, APT41 by FireEye, Blackfly and Suckfly by Symantec, Wicked Panda by CrowdStrike) linked to Chinese government interests.

These APT groups share an arsenal of malicious tools used in cyberespionage and financially motivated attacks since at least 2011.

That is when Kaspersky researchers discovered Winnti's Trojan malware on a massive number of compromised gaming systems following a supply chain attack that compromised a game's official update server.

Kaspersky also revealed evidence connecting Winnti attack tactics and methods used in the compromise of ASUS' LiveUpdate during Operation ShadowHammer to the ones employed in other supply-chain attacks, including NetSarang and CCleaner from 2017.

## APT groups increasingly target Linux users

The discovery of new is not at all surprising, taking into account the over 40% increase in new Linux malware found during 2020.

Nation-state hackers also focus more and more on targeting Linux systems, as highlighted by a 2020 Intezer report summarizing the last ten years of Linux APT attacks.

"In the previous decade researchers discovered several large APT campaigns targeting Linux systems, as well as unique Linux malware tools tailored for espionage operations," Intezer said.

"Some of the most prominent nation-state actors are incorporating offensive Linux capabilities into their arsenal and it's expected that both the number and sophistication of such attacks will increase over time."

Source: <https://www.bleepingcomputer.com/news/security/chinese-state-hackers-target-linux-systems-with-new-malware/>

## 6. Why MITRE ATT&CK Matters?

[MITRE ATT&CK enterprise](#) is a "knowledge base of adversarial [techniques](#)". In a Security Operations Center (SOC) this resource is serving as a progressive framework for practitioners to make sense of the *behaviors* (techniques) leading to system intrusions on enterprise networks. This resource is centered at how SOC practitioners of all levels can craft purposeful defense strategies to assess the *efficacy* of their security investments against that knowledge base.

To enable practitioners in operationalizing these strategies, the knowledge base provides the "*why*" and the "*what*" with comprehensive documentation that includes the descriptions and relational mappings of the behaviors observed by the execution of malware, or even when those weapons were used by known adversaries in their targeting of different victims as reported by security vendors. It goes a step further by introducing the "*how*" in the form of **adversary emulation plans** which streamline both the design of threat-models and the necessary technical resources to test those models – i.e., emulating the [behavior of the adversary](#)

For scenarios where SOC's may not have the capacity to do this testing themselves, the MITRE Corporation conducts annual evaluations of security vendors and their products against a carefully crafted adversary emulation plan, and it publishes the [results](#) for public consumption. The evaluations can help SOC teams assess both strategy concerns and tactical effectiveness for their defensive needs as they explore market solutions.

This approach is transformative for cyber security, it provides an effective way to evolve from constraints of being solely dependent on *IOC-centric* or *signature-driven* defense models to now having a behavior-driven capability for SOC's to tailor their strategic objectives into realistic security outcomes measured through *defensive efficacy* goals. With

a behavior-driven paradigm, the emphasis is on the value of **visibility** surrounding the events of a detection or prevention action taken by a security sensor – this effectively places context as the essential resource a defender must have available to pursue actionable outcomes.

## Cool! So what is this “efficacy” thing all about?

I believe that to achieve meaningful security outcomes our products (defenses) must demonstrate how effective they are (efficacy) at enabling or preserving the security mission we are pursuing in our organizations. For example, to view efficacy in a SOC, let’s see it as a foundation of 5 dimensions:

|                      |  |
|----------------------|--|
| <b>Detection</b>     | Gives SOC Analysts higher event actionability and alert handling efficiencies with a focus on most prevalent adversarial behaviors – i.e., let’s tackle the alert-fatigue constraint!                    |
| <b>Prevention</b>    | Gives SOC Leaders/Sponsors confidence to show risk reduction with minimized impact/severity from incidents with credible concerns – e.g., ransomware or destructive threats.                             |
| <b>Response</b>      | Gives SOC Responders a capacity to shorten the time between detection and activating the relevant response actions – i.e., knowing when and how to start containing, mitigating or eradicating.          |
| <b>Investigative</b> | Gives SOC Managers a capability to improve quality and speed of investigations by correlating low signal clues for TIER 1 staff and streamlining escalation processes to limited but advanced resources. |
| <b>Hunting</b>       | Enables SOC Hunters a capacity to rewind-the-clock as much as possible and expand the discovery across environments for high value indicators stemming from anomalous security events.                   |

## So how does “efficacy” relate to my SOC?

Efficacy at the Security and Technical Leadership levels confirms how the portfolio investments are expected to yield the defensive posture of our security strategy, for example, compare your investments today to any of the following:

| Strategy (Investment)   | Portfolio Focus   | Efficacy Goals   |
|---|-------------------|--|
|    | Balanced Security | <p><b>Ability to:</b></p> <ul style="list-style-type: none"> <li>• Focus on prevalent behaviors</li> <li>• Confidently prevent attack chains with relevant impact/severity</li> <li>• Provide alert actionability</li> <li>• Increase flexibility in response plans based on alert type and impact situation</li> </ul> <p><b>Caveats:</b></p> <ul style="list-style-type: none"> <li>• Needs efficacy testing program with adversary emulation plans</li> </ul>   |
|   | Detection Focus   | <p><b>Ability to:</b></p> <ul style="list-style-type: none"> <li>• Focus on prevalent behaviors</li> <li>• Provide alert actionability</li> <li>• Proactively discover indicators with hunting</li> </ul> <p><b>Caveats:</b></p> <ul style="list-style-type: none"> <li>• Requires humans</li> <li>• Minimal prevention maturity</li> <li>• Requires solid incident response expertise</li> <li>• Hard to scale to proactive phases due to prevention maturity</li> </ul>  |
|  | Prevention Focus  | <p><b>Ability to:</b></p> <ul style="list-style-type: none"> <li>• Confidently prevent attack chains with relevant impact/severity</li> <li>• Lean incident response plans</li> <li>• Provide alert actionability and Lean monitoring plans</li> </ul> <p><b>Caveats:</b></p> <ul style="list-style-type: none"> <li>• Hard to implement across the business without disrupting user experience and productivity</li> <li>• Typically for regulated or low tolerance network zones like PCI systems</li> <li>• Needs high TCO for the management of prevention products</li> </ul> |
|  | Response Focus    | <p><b>Ability to:</b></p> <ul style="list-style-type: none"> <li>• Respond effectively to different scenarios identified by products or reported to the SOC</li> </ul> <p><b>Caveats:</b></p> <ul style="list-style-type: none"> <li>• Always reacting</li> <li>• Requires humans</li> <li>• Hard to retain work staff</li> <li>• Unable to spot prevalent behaviors</li> <li>• Underdeveloped detection</li> <li>• Underdeveloped prevention</li> </ul>   |



MITRE ATT&CK matters as it introduces the practical sense-making SOC professionals need so they can discern attack chains versus security events through visibility of the most prevalent behaviors.

Consequently, it allows practitioners to overcome crucial limitations from the reliance on indicator-driven defense models that skew realistic efficacy goals, thereby maximizing the value of a security portfolio investment.

Source: <https://www.mcafee.com/blogs/enterprise/security-operations/why-mitre-attck-matters/>

## 7. Phishing sites now detect virtual machines to bypass detection

Phishing sites are now using JavaScript to evade detection by checking whether a visitor is browsing the site from a virtual machine or headless device.

Cybersecurity firms commonly use headless devices or virtual machines to determine if a website is used for phishing.

To bypass detection, a phishing kit utilizes JavaScript to check whether a browser is running under a virtual machine or without an attached monitor. If it discovers any signs of analysis attempts, it shows a blank page instead of displaying the phishing page.

Discovered by [MalwareHunterTeam](#), the script checks the visitor's screen's width and height and uses the WebGL API to query the rendering engine used by the browser.

```
var canvas = document.createElement('canvas');
var gl = canvas.getContext('webgl');
var debugInfo = gl.getExtension('WEBGL_debug_renderer_info');
var vendor = gl.getParameter(debugInfo.UNMASKED_VENDOR_WEBGL);
var renderer = gl.getParameter(debugInfo.UNMASKED_RENDERER_WEBGL);
console.log(vendor);
console.log(renderer);
var width = screen.width;
var height = screen.height;
var color_depth = screen.colorDepth;
```

### Using APIs to get renderer and screen info

When performing the checks, the script will first see if the browser uses a software renderer, such as [SwiftShader](#), [LLVMpipe](#), or VirtualBox. Software renderers commonly indicate that the browser is running within a virtual machine.

The script also checks if the visitor's screen has a color depth of less than 24-bits or if the screen height and width are less than 100 pixels, as shown below.

```
setTimeout(function() {  
  if (true) {  
  
    // seems we use data above to check render!  
  
    if (/swiftshader/i.test(renderer.toLowerCase()) || /llvmpipe/i.test(renderer.toLowerCase()) ||  
    /virtualbox/i.test(renderer.toLowerCase()) || !renderer) {  
  
      // blacklist!  
      console.log("Virtual Machine / RDP");  
    }  
  
    else if (color_depth < 24 || width < 100 || width < 100 || !color_depth) {  
  
      alert('bot detected')  
  
      console.log("No Display (Probably Bot)")  
    }  
  
    else {  
      $.get("m3dularbh/ajax.php?n=m3d", function(data, status){ window.location.href = 'main/';});  
      // document ready  
    }  
  }  
}
```

### Performing checks for virtual machines and headless devices

If it detects any of these conditions, the phishing page will display a message in the browser's developer console and show an empty page to the visitor.

However, if the browser uses a regular hardware rendering engine and a standard screen size, the script will display the phishing landing page.

The code used by this threat actor appears to have been taken from a [2019 article](#) describing how JavaScript can be used to detect virtual machines.

[Fabian Wosar](#), CTO of cybersecurity firm Emsisoft, told BleepingComputer that security software utilize a variety of methods to scan for and detect phishing sites. These include signature matching and visual machine using machine learning.

"Code like the one above actually will work for some of these techniques. However, it is also trivial to prevent by just hooking a couple of JavaScript APIs and providing "fake" information," Wosar explained.

As it's common for researchers and security companies to harden their virtual machines to evade detection by malware, it appears they will now also have to harden them against phishing attacks.

As a way to see what renderer and screen information is reported by your browser, BleepingComputer has created a [test page](#) that you can use.

Source: <https://www.bleepingcomputer.com/news/security/phishing-sites-now-detect-virtual-machines-to-bypass-detection/>

## 8. The Week in Ransomware - March 19th 2021 - Highest ransom ever!

While the beginning of this week was fairly quiet, it definitely ended with a bang as news came out of the largest ransom demand yet.

It was revealed at the end of the week that computer maker [Acer suffered a REvil ransomware attack](#) where the threat actors are demanding a massive \$50,000,000 ransom.

REvil also made this news this week with the addition of a [new -smode argument](#) that causes Windows to reboot into Safe Mode with Networking to perform the encryption. REvil's 'Unknown' also [conducted an interview](#) with TheRecord.

Finally, we saw an [FBI warning about PYSA](#) and new variants of ransomware families released.

Contributors and those who provided new ransomware information and stories this week include: [@malwareforme](#), [@struppigel](#), [@LawrenceAbrams](#), [@Seifreed](#), [@DanielGallagher](#), [@VK Intel](#), [@fwosar](#), [@malwrhunterteam](#), [@FourOctets](#), [@demonslay335](#), [@BleepinComputer](#), [@serghei](#), [@jorntvdw](#), [@Ionut Ilascu](#), [@PolarToffee](#), [@Amigo A](#), [@GrujaRS](#), [@ddd1ms](#), [@campuscodi](#), [@ValeryMarchive](#), [@3xp0rtblog](#), [@Kangxiaopao](#), and [@fbgwls245](#).

### March 13th 2021

#### **New RunExeMemory ransomware variant**

[GrujaRSA](#) found a new variant of the RunExeMemory that appends the .z8sj2c extension and drops a ransom note named Read me, if you want to recover your files.txt.

### March 16th 2021

#### **FBI warns of escalating Pysa ransomware attacks on education orgs**

The Federal Bureau of Investigation (FBI) Cyber Division has warned system administrators and cybersecurity professionals of increased Pysa ransomware activity targeting educational institutions.

#### **An interview with REvil's Unknown**

Unknown talked to Recorded Future expert threat intelligence analyst Dmitry Smilyanets recently about using ransomware as a weapon, staying out of politics, experimenting with new tactics, and much more. The interview was conducted in Russian and translated to English with the help of a professional translator, and has been edited for clarity.

#### **New Liz Dharma ransomware variant**

[Jakub Kroustek](#) found a new Dharma Ransomware variant that appends the .liz extension.

#### **New Rapid ransomware variant**

[dnwls0719](#) found a new Rapid ransomware variant that appends the .lock extension.

#### **New Xorist ransomware variant**

[xiaopao](#) found a new variant of the Xorist ransomware that appends the .sandboxtest extension.

## **March 17th 2021**

### **Missed opportunity: Bug in LockBit ransomware allowed free decryptions**

A member of the cybercriminal community has discovered and disclosed a bug in the LockBit ransomware that could have been used for free decryptions.

#### **New Hakbit ransomware variant**

xiaopao found a new variant of the Hakbit ransomware that appends the **.PROM** extension.

#### **New SFile ransomware variant**

xiaopao found a new variant of the SFile ransomware that appends the **.zuadr** extension and drops a ransom note named **RESTORE\_FILES\_INFO.hta** and **RESTORE\_FILES\_INFO.txt**.

## **March 18th 2021**

#### **New PewPew Ransomware variant**

[Amigo-A](#) found a new PewPew Ransomware variant that calls itself 'Artemis' and appends the **.optimus** extension to encrypted files.

#### **New Stop ransomware variant**

dnwls0719 found a new STOP Djvu ransomware variant that appends the **.enfp** and drops a ransom note named **\_readme.txt**.



**ATTENTION!**

Don't worry, you can return all your files!  
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.  
The only method of recovering files is to purchase decrypt tool and unique key for you.  
This software will decrypt all your encrypted files.  
What guarantees you have?  
You can send one of your encrypted file from your PC and we decrypt it for free.  
But we can decrypt only 1 file for free. File must not contain valuable information.  
You can get and look video overview decrypt tool:  
<https://we.tl/t-NuEqGxqRg2>  
Price of private key and decrypt software is \$980.  
Discount 50% available if you contact us first 72 hours, that's price for you is \$490.  
Please note that you'll never restore your data without payment.  
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:  
[helpteam@mail.ch](mailto:helpteam@mail.ch)

Reserve e-mail address to contact us:  
[helpmanager@airmail.cc](mailto:helpmanager@airmail.cc)

Your personal ID:  
0288Widasdgy4Hld4Nu8hMhno9C8AEpO10FUGAYGVNmXbgsUt1

## March 19th 2021

### REvil ransomware has a new 'Windows Safe Mode' encryption mode

The REvil ransomware operation has added a new ability to encrypt files in Windows Safe Mode, likely to evade detection by security software and for greater success when encrypting files.

### Computer giant Acer hit by \$50 million ransomware attack

Electronics giant Acer has been hit by a REvil ransomware attack where the threat actors are demanding the largest known ransom to date, \$50,000,000.

### Cyberattaque : une rançon de 50 millions de dollars demandée à Acer

Les opérateurs du rançongiciel Revil, aussi connu sous le nom Sodinokibi, ont ajouté le constructeur à la liste de victimes. Ils laissent encore près de 9 jours à Acer pour négocier, faute de quoi ils doubleront leurs exigences.

### Ransomware statistics for 2020: Year in summary

2020, the year of the pandemic, was another lucrative year for ransomware. As nations around the world scrambled to slow the spread of the virus, cybercriminals attempted to capitalize on the chaos.

### New SFile ransomware variant

xiaopao found a new variant of the SFile ransomware that appends the **.Technomous-zbtrqyd** extension.

Source: <https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-19th-2021-highest-ransom-ever/>

## 9. Microsoft warns of phishing attacks bypassing email gateways

An ongoing phishing operation that stole an estimated 400,000 OWA and Office 365 credentials since December has now expanded to abuse new legitimate services to bypass secure email gateways (SEGs).

The attacks are part of multiple phishing campaigns collectively dubbed [the "Compact" Campaign](#), active since early 2020 first detected by the WMC Global Threat Intelligence Team.

"Phishers continue to find success in using compromised accounts on email marketing services to send malicious emails from legitimate IP ranges and domains," Microsoft's security experts [said](#).

"They take advantage of configuration settings that ensure delivery of emails even when the email solution detects phishing."

Appspot now also abused to bypass SEGs

Attackers behind these phishing campaigns have stolen more than 400,000 stolen Office 365 and Outlook Web Access credentials since December, according to WMC Global.

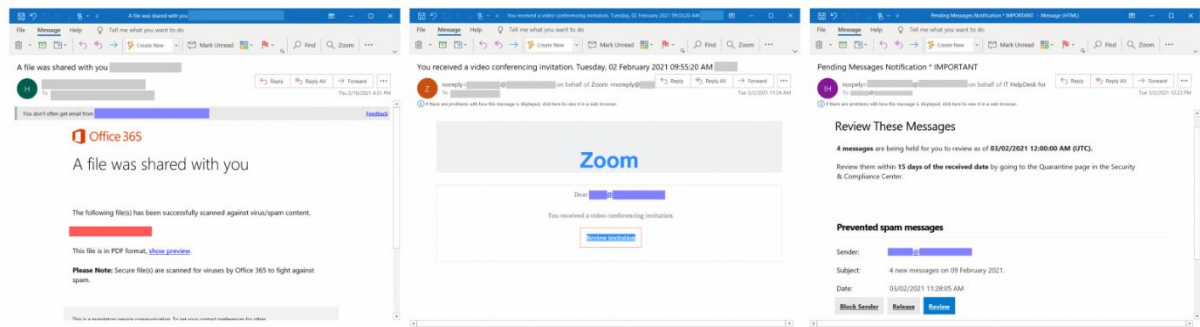
Their phishing emails are camouflaged as notifications from video conferencing services, various security solutions, and productivity tools to add legitimacy.

The threat actors also use compromised accounts for SendGrid and MailGun email delivery services, taking advantage of secure email gateways allow lists having them listed as trusted domains.

This allows the phishing messages to bypass them and land in the targets' inboxes, luring them into clicking on embedded hyperlinks that redirect them to phishing landing pages designed to impersonate Microsoft login pages.

"In December, the landing page impersonated the Outlook Web App brand to trick targets into entering their credentials," WMC Global said.

"In January, the attacks changed to mimic Office 365 brand, likely to capture more employee credentials."



## Spooled emails (Microsoft)

The phishing operation continues to expand as it now also abuses Amazon Simple Email Service (SES) and the Appspot cloud computing platform—used to develop and host web apps in Google-managed data centers—to deliver phishing emails and generate multiple phishing URLs for each target.

Domains and accounts used throughout this phishing campaign are being taken down as soon as Microsoft and WMC Global detect them.

"We shared our findings with Appspot, who confirmed the malicious nature of the reported URLs and used the shared intelligence to find and suspend additional offending projects on Appspot," Microsoft added.

"Because this campaign uses compromised email marketing accounts, we strongly recommend orgs to review mail flow rules for broad exceptions that may be letting phishing emails through," Microsoft [advised](#).

Source: <https://www.bleepingcomputer.com/news/security/microsoft-warns-of-phishing-attacks-bypassing-email-gateways/>

## 10. Microsoft improves Windows Sandbox in latest Windows 10 build

The Windows Sandbox and the Microsoft Defender Application Guard (WDAG) now launch faster in Windows 10 after installing the Insider Preview Build 21343 for Windows Insiders in the Dev Channel.

Windows Sandbox helps Windows 10 users safely run apps in an isolated desktop environment. MDAG blocks old and newly emerging attacks using a hardware isolation approach powered by Hyper-V-enabled containers.

"Starting with Build 21343, we are introducing a new runtime that is designed and optimized for container scenarios," Windows Insider Program senior program manager Brandon LeBlanc said.

"It is lightweight and allows faster launch times for both Windows Sandbox and Microsoft Defender Application Guard."

This change should not impact application compatibility in any way within Windows Sandbox containers, but Microsoft is expecting some behavior changes.

Microsoft also introduced new File Explorer icons, with multiple system icons used throughout the file manager now updated to a new look.

The new Chromium-based Edge is now the default web browser after replacing Edge Legacy, starting with Build 21313. The new Edge browser was officially released in January 2020 with an installer that replaces the legacy version.

Edge Legacy will be permanently removed and replaced in all Windows 10 builds with the new Microsoft Edge by April's Windows 10 Patch Tuesday security update.

## Changes and Improvements:

- We're changing the name of the Windows Administrative Tools folder in Start to Windows Tools. We are working to better organize all the admin and system tools in Windows 10.
- [News and interests] Update on the rollout: following our last update on languages and markets, this week we're also introducing the experience to China! We continue to roll out news and interests to Windows Insiders, so it isn't available to everyone in the Dev Channel just yet.
- We are now rolling out the new IME candidate window design to all Windows Insiders in the Dev Channel using Simplified Chinese IMEs.
- We're updating the "Get Help" link in the touch keyboard to now say "Learn more".
- We're updating File Explorer when renaming files to now support using CTRL + Left / Right arrow to move your cursor between words in the file name, as well as CTRL + Delete and CTRL + Backspace to delete words at a time, like other places in Windows.
- We've made some updates to the network related surfaces in Windows so that the displayed symbols use the updated system icons we recently added in the Dev Channel.
- Based on feedback, if the Shared Experiences page identifies an issue with your account connection, it will now send the notifications directly into the Action Center rather than repeated notification toasts that need to be dismissed.



## Fixes:

- We fixed an issue where devices with certain NVMe drives were experiencing disk resets or WHEA\_UNCORRECTABLE\_ERROR bugchecks.
- We fixed an issue where some devices were receiving DPC\_WATCHDOG\_ERROR bugchecks.
- We fixed an issue where some devices with Realtek network adapters running driver version 1.0.0.4 were experiencing intermittent loss of network connectivity.
- [News and interests] Fixed an issue where on some occasions the news and interests button text was using the wrong high contrast color.
- [News and interests] Fixed an issue where news and interests may not be available when signing into Windows without internet access but returns when online.
- [News and interests] We've made multiple fixes to help improve performance and reliability for explorer.exe.
- We fixed an issue resulting in explorer.exe crashing with Event ID 1002.
- We fixed a memory leak when interacting with the Recycle Bin.
- We fixed a deadlock in recent Dev Channel builds related to the Indexer, which could result in not being able to launch Start menu or other apps on first boot after an upgrade.
- We fixed an issue where on some high-refresh-rate monitors, games would only run at 60Hz. This issue may have also resulted in tearing in variable-refresh-rate monitor scenarios.
- We fixed an underlying issue resulting in some apps crashing during install and potentially other activities recently.
- We fixed an underlying issue resulting in some apps unexpectedly displaying a message saying, "You must restart your computer before the new settings will take effect." recently.
- We fixed an issue resulting in blurry text on secondary monitors in recent Dev Channel build when the monitor was set to portrait orientation.
- We fixed an issue impacting the reliability of WIN + Shift + Left / Right Arrow in recent builds.
- We fixed an issue where the size information for large capacity drives could be truncated in File Explorer's properties dialog.
- We fixed an issue that could result in the header at the top of Settings having truncated text in some languages.

- We made a fix to help address an issue where the user profile picture in the Settings header would flicker when resizing the window. Please let us know if you're still noticing this after upgrading.
- We fixed an issue where after changing audio end points the volume controls in Sound Settings might stop working.
- We fixed an issue where the Properties and Data Usage options were missing in Network Status settings page recently.
- We fixed an issue where if you searched for "Advanced touchpad gesture configuration" and clicked the result, it would just launch Settings, and not that specific Settings page.
- We fixed an issue resulting in Settings crashing for some Insiders after launching it by double clicking on the Windows Update icon in the taskbar.
- We fixed an issue that was blocking Azure Data Studio from updating to a newer version on ARM64.
- We fixed issues that were causing Ngen.exe to fail to precompile .NET Framework binaries on ARM64.
- We fixed an issue that could result in some of the touch keyboard's child keys being cut off.
- We fixed an issue where a flick up on the top row of the touch keyboard wouldn't insert the corresponding number when using the small touch keyboard layout, unlike the other layouts.
- We fixed an issue that could result in display issues with the IME candidate windows after switching between light and dark theme.
- We fixed an issue where after typing a very long string of text the Japanese IME could become disabled.
- We fixed an issue where it wasn't possible to use SHIFT + Space in Excel when typing with the Japanese IME.
- We fixed an issue with the Japanese IME where it wasn't possible to enter a sentence that began with "を" when typing in Kana input mode.

Source: <https://www.bleepingcomputer.com/news/microsoft/microsoft-improves-windows-sandbox-in-latest-windows-10-build/>

## 11. Engineer reports data leak to nonprofit, hears from the police

A security engineer and ex-contributor to an open systems non-profit organization recently reported a data leak to the organization.

In return, he first got thanked for his responsible reporting, but later heard from their lawyers and the police.

Apperta Foundation is a UK-based non-profit, supported by NHS England and NHS Digital, that promotes open systems and standards in the digital health and social care space.

### GitHub repository exposed passwords, keys, database

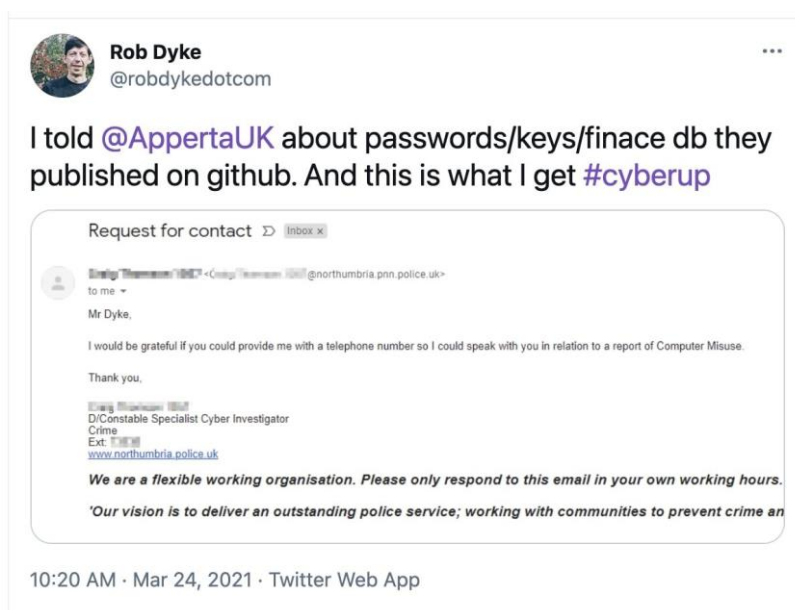
This week, a British cloud security engineer Rob Dyke spoke out on how an instance of ethically reporting a data leak landed him in legal trouble.

Earlier this month, Dyke had discovered an exposed GitHub repository exposing passwords, API keys, and sensitive financial records which belonged to Apperta Foundation.

On discovering this GitHub repository which, the engineer says, was public since at least 2019, the engineer privately reported it to Apperta, and got thanked by them.

On March 9th, however, he received legal correspondence from Apperta's lawyers, leading him to hire his own solicitors to represent him.

Furthermore, an email followed yesterday from a Northumbria Police cyber investigator in relation to a report of "Computer Misuse."



### Security engineer Rob Dyke receives an email from Northumbria Police

Source: [Twitter](#)

In a phone interview with BleepingComputer, Dyke told us that having worked with Apperta in the past [1, 2, 3] and as someone currently working in the IT sector, he's very familiar with both Apperta's established mechanism and the industry practices when it comes to responsibly reporting security vulnerabilities to vendors.

When he came across the data leak, Dyke had immediately reported it to Apperta.

To have a record of what he had reported, however, the researcher encrypted the data he had come across and securely stored it aside for 90 days, as a part of the coordinated disclosure process.

"I knew how I was supposed to report it to them. So I reported it to them, via their established procedure," the engineer told BleepingComputer further adding that he had received a reply from Apperta with the representative thanking him, and stating they'll get the issue sorted.

"And I didn't really think any more about it," Dyke continued.

A little over a week later, a letter arrived from Apperta's lawyers stating that they considered Dyke's actions as "unlawful" and demanded a written undertaking that any data the engineer had come across was deleted.

This left the engineer surprised especially considering that Apperta team members knew him from his past contributions.

In emails seen by BleepingComputer, Dyke further clarified to Apperta's lawyers that the information he came across was being leaked on GitHub publicly for over two years, rather than proprietary data obtained as a part of unlawful hacking activity.

The details gathered by the engineer as a part of the responsible disclosure was done so from openly accessible public URLs published by Apperta on the internet.

Dyke further issued a written affirmation that he will destroy any copy of the repository obtained from the public web service (GitHub) and provide a certificate of destruction.

Yesterday, another letter arrived from the Northumbria Police station inquiring more details about what the police refers to a report of "Computer Misuse (Act)."

The engineer told BleepingComputer he believes the police investigation is linked to the Apperta incident, given that Northumbria Police oversees the jurisdiction where Apperta's offices are located.

"I don't think this is the way to go about it for an organization that's promoting openness, and, all of the things that go with that; transparency, accountability, and responsibility."

"Since I've found this leak, and helped them out, this is simply not the way to go about it. I gave [them] assurance that the data will be deleted, and it has been deleted," Dyke further explained to BleepingComputer.

## UK Computer Misuse Act scares away 80% of infosec professionals

This is not the first time an information security engineer has allegedly stepped into the legal gray area of UK's Computer Misuse Act (CMA).

**The Register** has repeatedly [1, 2, 3] tracked developments on Computer Misuse Act and why time and time again both British infosec. firms and academics have urged that aspects of the dated law be reformed.

A study conducted by the CyberUp campaign stated that 80% of security professionals were scared of falling foul of Computer Misuse Act during course of their routine professional activities.

The provisions of the [UK Computer Misuse Act of 1990](#) are vast and extensive and may even consider simply coming across a data leak as an "offence."

Even work activities of UK-based threat intelligence providers probing **foreign** systems may be considered illegal under the Act.

BleepingComputer reached out to Apperta Foundation multiple times and Northumbria Police well in advance for comment, but we have not heard back.

Source: <https://www.bleepingcomputer.com/news/security/engineer-reports-data-leak-to-nonprofit-hears-from-the-police/>



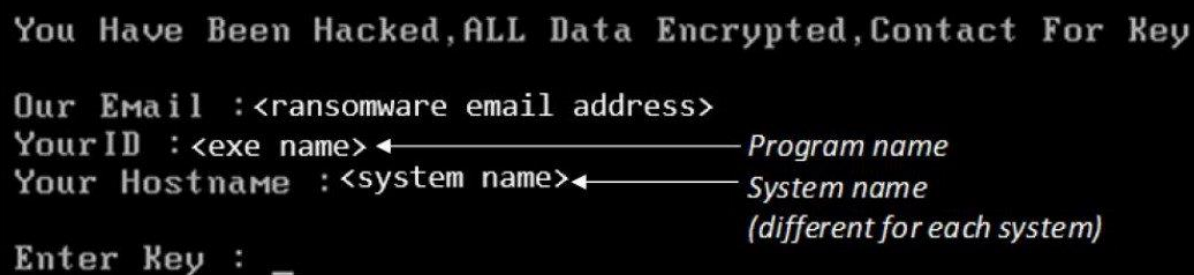
## 12. FBI exposes weakness in Mamba ransomware, DiskCryptor

An alert from the U.S. Federal Bureau of Investigation about Mamba ransomware reveals a weak spot in the encryption process that could help targeted organizations recover from the attack without paying the ransom.

The FBI warns that Mamba ransomware attacks have been directed at entities in the public and private sector, including local governments, transportation agencies, legal services, technology services, industrial, commercial, manufacturing, and construction businesses.

### Race to get the encryption key

Mamba ransomware (a.k.a. HDDCryptor) relies on an open-source software solution named DiskCryptor to encrypt victim computers in the background with a key defined by the attacker.



```
You Have Been Hacked, ALL Data Encrypted, Contact For Key

Our Email : <ransomware email address>
Your ID : <exe name> ← Program name
Your Hostname : <system name> ← System name
                                   (different for each system)
Enter Key : _
```

The FBI explains that installing DiskCryptor requires a system restart to add necessary drivers, which occurs with Mamba approximately two minutes after deploying the program.

The agency further notes that the encryption key and the shutdown time variable are stored in DiskCryptor's configuration, a plaintext file named myConf.txt.

A second restart of the system happens once the encryption process completes, around two hours later, and the ransom note becomes available.

Because there is no protection around the encryption key, as it is saved in plaintext, the FBI says that this two-hour gap is an opportunity for organizations hit by Mamba ransomware to recover it.

"If any of the DiskCryptor files are detected, attempts should be made to determine if the myConf.txt is still accessible. If so, then the password can be recovered without paying the ransom. This opportunity is limited to the point in which the system reboots for the second time" - [the FBI](#)

The Mamba ransomware operation started to increase its activity with a new variant found in the second half of 2019. Despite not having an affiliate program, it was among the top threats.

In a [report from Coveware](#), in the first quarter of last year Mamba was sitting in the top five ransomware threats led by REvil and Ryuk. This changed in the fourth quarter of 2020, although it continued to be a [notable risk](#).

One peculiarity of Mamba ransomware is that it overwrite the disk's master boot record (MBR), preventing access to encrypted files on the drive. This makes it more difficult to track the number of attacks since files cannot be analyzed through automated services like [ID-Ransomware](#).

The FBI provides the following details on artifacts that could help organizations detect a Mamba ransomware attack:

| Key Artifacts                          |   |
|--|---|
| Files                                  | Description   |
| \$dcsys\$                              | Located in the root of every encrypted drive [i.e. C:\\$dcsys\$]  |
| C:\Users\Public\myLog.txt              | Ransomware log file   |
| C:\Users\Public\myConf.txt             | Ransomware configuration file   |
| C:\Users\Public\dcapi.dll              | DiskCryptor software executable   |
| C:\Users\Public\dcinst.exe             | DiskCryptor software executable   |
| C:\Users\Public\dccon.exe              | DiskCryptor software executable   |
| C:\Users\Public\dcrypt.sys             | DiskCryptor software executable   |
| C:\Windows\System32\Drivers\dcrypt.sys | Installed DiskCryptor driver  |
| [Ransomware Filename].exe              | Portable 32-bit .NET assembly compatible with 32-bit and 64-bit Windows systems which combines DiskCryptor with a simple ransom message upon boot |

|   |                                |
|---|--------------------------------|
| dcinst.exe  | Cryptor installer support      |
| dccon.exe   | Console version of DiskCryptor |
| Services  |                                |
| myCryptoraphyService  |                                |
| Runs [Ransomware Filename].exe as a service and is removed once encryption is completed |                                |

Source: <https://www.bleepingcomputer.com/news/security/fbi-exposes-weakness-in-mamba-ransomware-diskcryptor/>

## 13. Ransomware admin is refunding victims their ransom payments

After recently announcing the end of the operation, the administrator of Ziggy ransomware is now stating that they will also give the money back.

It appears that this is a planned move since the admin shared the "good news" a little over a week ago, but gave no details.

### Shutdown followed by money-back move

Ziggy ransomware shut down in early February. In a short announcement, the administrator of the operation said that they were "sad" about what they did and that they "decided to publish all decryption keys."

They followed through the next day, on February 7, offering an SQL file with [922 decryption](#) keys that victims could use to unlock their files.

The admin also made available a decryption tool to make the process easier, along with the source code for a decryptor that does not need an internet connection to work.

On March 19, the Ziggy ransomware administrator said that they also wanted to return the money to the victims that paid the ransom. Today, after a week of silence, the admin said that they were ready to revert payments.

Victims should contact the admin at a given email address (ziggyransomware@secmail.pro) with the proof of their payment in bitcoin and the

computer ID, and the money would be returned to the victim's bitcoin wallet in about two weeks.

Friday, March 19, 2021



#### Ziggy Ransomware Decrypted

68 11:48:07 PM

Good news

We have a plane to return victims money.

Sunday, March 28, 2021



#### Ziggy Ransomware Decrypted

30 edited 1:09:26 PM

If you are infected with Ziggy ransomware and your payed money, We are ready to give back your money.

Send you payment receipt and your computer unique ID to this E-mail :

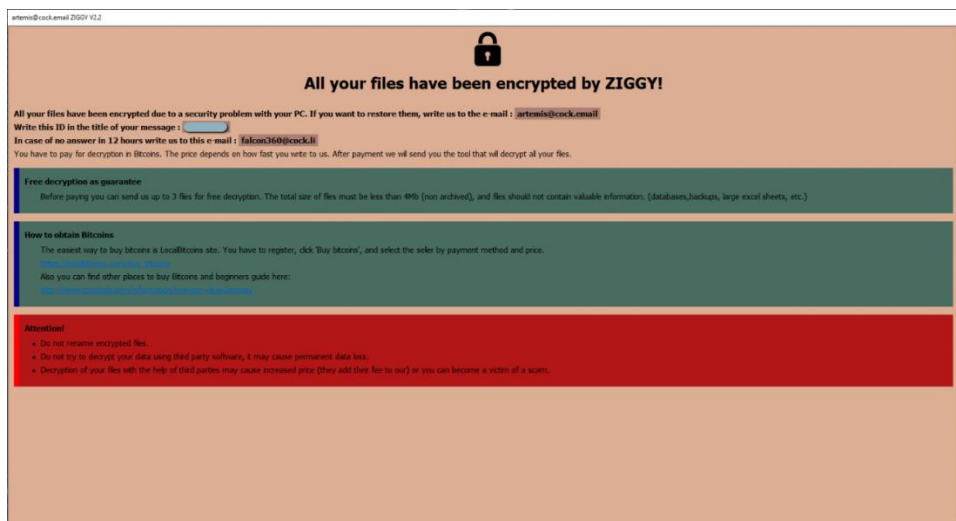
[ZiggyRansomware@secmail.pro](mailto:ZiggyRansomware@secmail.pro)

We Will transfer money to your Bitcoin wallet address.

we will give back your money until 2 weeks later.

## Returning the ransom and making a profit

Ransomware victims get a ransom note with instructions on how to contact cybercriminals to negotiate a payment. Typically, the payment is negotiated in fiat but paid in Bitcoin.



source: [Michael Gillespie](#)

Speaking to BleepingComputer, the administrator of Ziggy ransomware said that the refund will be in Bitcoin at the value on payment day.

Bitcoin price has been on ascending route for the past three months, and its price at the moment of writing is close to \$55,000.

On the day Ziggy ransomware decryption keys became public, Bitcoin price was around \$39,000. Five days before the admin announced that they would return the money, Bitcoin spiked above \$61,000. Given the price difference, the admin makes a profit at the current Bitcoin price.

The Ziggy ransomware administrator told BleepingComputer that they lived in a “third-world country” and that their motivation for creating the locker was financial. They confirmed to us that the recent actions are driven by fear of law enforcement getting them. Recent activity that disrupted much larger operations like [Emotet](#) and [Netwalker ransomware](#) likely weighed a lot towards this decision.

The admin also claims that they had to sell their house to be able to refund Ziggy ransomware victims and that they plan to switch sides and become a ransomware hunter after returning the money.

**Update [March 29, 11:14 EST]:** Article updated with information from the administrator of Ziggy ransomware.

Source: <https://www.bleepingcomputer.com/news/security/ransomware-admin-is-refunding-victims-their-ransom-payments/>

## 14. Microsoft Exchange attacks increase while WannaCry gets a restart

The recently patched vulnerabilities in Microsoft Exchange have sparked new interest among cybercriminals, who increased the volume of attacks focusing on this particular vector.

While ransomware attacks have increased in frequency in the past six months, cybersecurity company Check Point last week noticed a surge in incidents targeting Microsoft Exchange servers vulnerable to the so-called ProxyLogon critical bugs.

Even with patching moving at a rapid pace, the company saw attempted attacks triple across the globe, counting tens of thousands.



## Microsoft Exchange still attractive

According to Microsoft, there were about 82,000 [vulnerable Exchange servers](#) on March 14. About a week later, the number dropped considerably to roughly 30,000 exposed machines, as per data from RiskIQ.

Telemetry data from Check Point last week showed more than 50,000 attack attempts globally, most of them aimed at organizations in the government/military, manufacturing, and banking/finance sectors.

Almost half of the exploit attempts occurred in the U.S. (49%), by far the most appealing region compared to other countries where Check Point recorded far fewer incidents (UK - 5%, Netherlands and Germany - both 4%).

## Ransomware attacks go up, WannaCry still a problem

The company saw a 57% rise in ransomware attacks over the past six months at a global level. More worrisome is a constant monthly increase of 9% since the beginning of the year.

Aside from the normal ransomware strains observed (Maze, Ryuk, REvil), the company notes a 53% swell in the number of organizations affected by the wormable WannaCry ransomware.

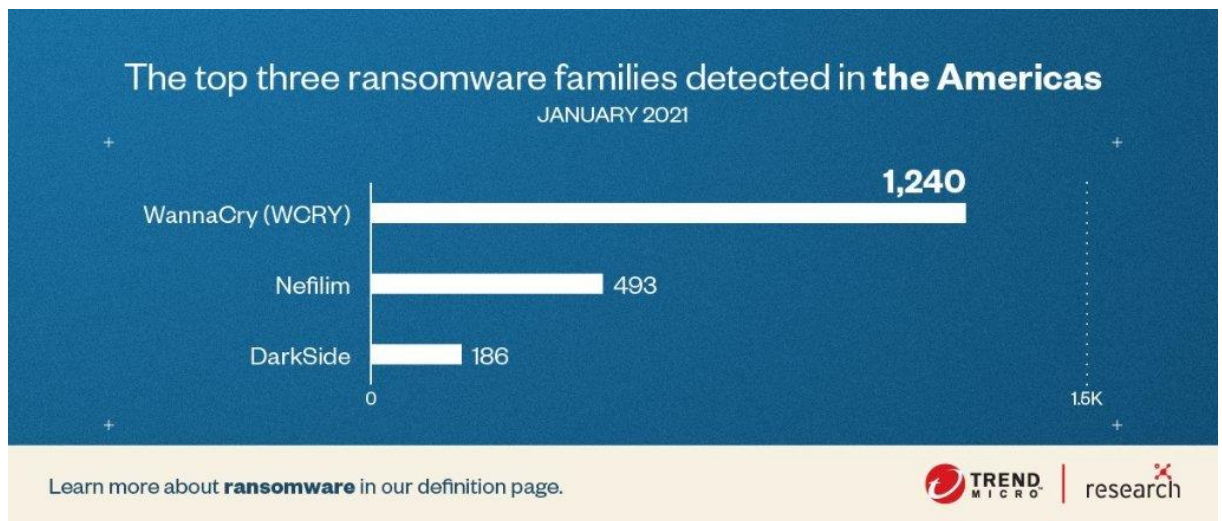
"In fact, CPR found that there are 40 times more affected organizations in March 2021 when compared to October 2020. The new samples still use the EternalBlue exploit to propagate – for which patches have been available for over 4 years" - [Check Point](#)

Almost four years ago, the [WannaCry outbreak](#) propagated through NSA's EternalBlue for Windows Server Message Block (SMB), causing hundreds of millions of USD in damages in just a few days.

Its spread was contained after security researcher [Marcus Hutchins discovered a kill switch](#) and Microsoft released [patches](#). Over 200,000 computers were affected by the attacks.

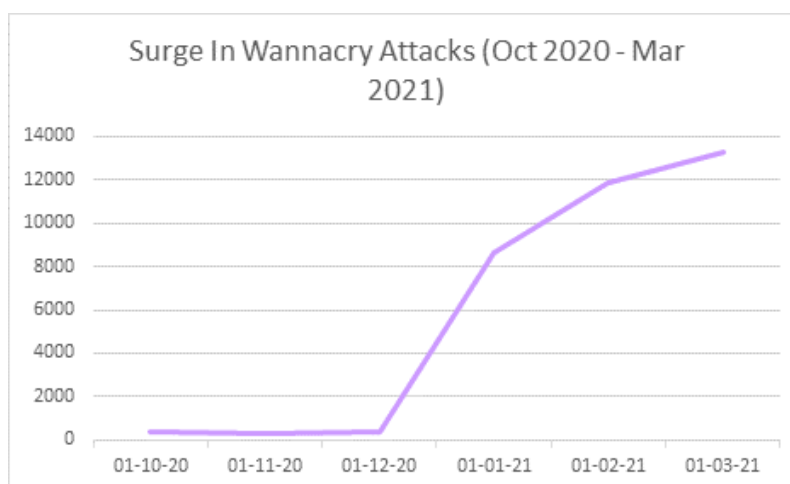
The malware has not been eradicated, though. Security firms continue to detect WannaCry even these days. These detections are for variants of the original WannaCry that have been modified to ignore the kill switch. Furthermore, security researcher [Vesselin Bontchev says](#) that he never found a sample with a working ransomware component.

In January, these WannaCry variants represented TrendMicro's top ransomware detection.



The reason behind the high numbers is WannaCry being wormable and thousands of systems still vulnerable to EternalBlue that are reachable over the public internet.

Check Point observed the same trend starting in December 2020, with attacks continuing to increase well over 12,000 in March 2021.



The figures show the importance of patching on time, else organizations remain vulnerable to attack vectors that should be mostly extinct.

**Update [March 31, 2021]:** Article updated to clarify that the WannaCry detections are not for the original variant of the malware used in the 2017 global outbreak.

Source: <https://www.bleepingcomputer.com/news/security/microsoft-exchange-attacks-increase-while-wannacry-gets-a-restart/>

## 15. Malicious Docker Cryptomining Images Rack Up 20M Downloads

Publicly available cloud images are spreading Monero-mining malware to unsuspecting cloud developers.

At least 30 malicious images in Docker Hub, with a collective 20 million downloads, have been used to spread cryptomining malware, according to an analysis.

The malicious images (spread across 10 different Docker Hub accounts) have raked in around \$200,000 from cryptomining, according to Aviv Sasson, researcher with Palo Alto Networks' Unit 42, who found and reported the malicious activity.

The most popular cryptocurrency in the instances observed by Sasson was Monero, which accounted for around 90 percent of the activity. Monero not only provides "maximum anonymity," as Sasson explained in a recent [blog posting](#), due to its hidden transaction paths – but it's also easier to mine cost-effectively. Monero crypto-operations can run on any machine, unlike, say, Bitcoin, which can require something like a GPU with its better processing speed to mine economically.

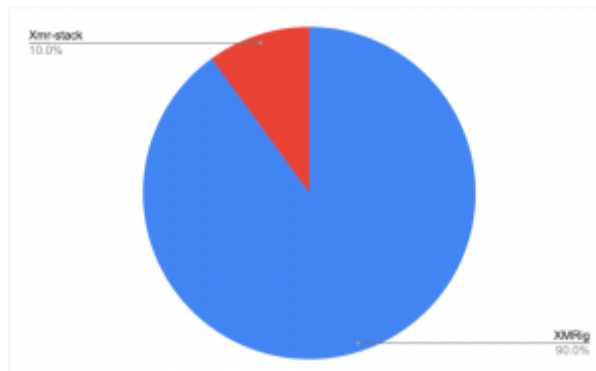
In most attacks that mine Monero, the attackers used the [well-worn XMRig](#) off-the-shelf miner, Sasson found.

"XMRig is a popular Monero miner and is preferred by attackers because it's easy to use, efficient and, most importantly, open source," he explained. "Hence, attackers can modify its code. For example, most Monero cryptominers forcibly donate some percentage of their mining time to the miner's developers. One common modification attackers make is to change the donation percentage to zero."

Two other cryptocurrencies were found in the mining pools: Grin, accounting for 6.5 of the activity, and Arionum, accounting for 3.2 percent.

## Public Images Serve Up Tailored Cryptojacking

In this case, malware is spread through the cloud via trojanized images that were publicly available within the Docker Hub container registry, for use in building cloud applications. Just as is the case with public code repositories [like npm](#) or Ruby, anyone can upload images to a Docker Hub account.



**Distribution of Monero-miners. Click to enlarge. Source: Unit 42.**

Sasson found that the adversaries behind the malicious images have applied tags to them, which are a way to reference different versions of the same image. He theorized that the tags are used to match up the appropriate version of the malware depending on which version of the image that the application pulls in.

"When examining the tags of the images, I found that some images have different tags for different CPU architectures or operating systems," he explained. "It seems like some attackers are versatile and add these tags in order to fit a broad range of potential victims that includes a number of operating systems (OS) and CPU architectures. In some images, there are even tags with different types of cryptominers. This way, the attacker can choose the best cryptominer for the victim's hardware."

## Shared Mining Pools Link Campaigns

Interestingly, the researcher was able to link the tags back to specific wallet addresses, which allowed him to classify campaigns.

"After digging deeper, in some cases, I could see that there are numerous Docker Hub accounts that belong to the same campaign," he explained. "For example, in previous research, Unit 42 found the malicious account `azurenql`. Now, we discovered that the campaign is broader and includes the accounts `021982`, `dockerxmrig`, `ggcloud1` and `ggcloud2`."

It's very possible that the images that Sasson discovered are merely the tip of the iceberg, given that the cloud presents big opportunities for cryptojacking attacks.

"It is reasonable to assume that there are many other undiscovered malicious images on Docker Hub and other public registries," he said. "In my research, I used a cryptomining scanner that only detects simple cryptomining payloads. I also made sure any identified image was malicious by correlating the wallet address to previous attacks. Even with these simple tools, I was able to discover tens of images with millions of pulls. I suspect that this phenomenon may be bigger than what I found, with many instances in which the payload is not easily detectable."

## Docker Under Fire

Docker-based cryptojacking and malware attacks have been on the rise [since at least 2018](#), largely because of the amount of horsepower for mining operations that the cloud can deliver, Sasson explained.

"The cloud consists of many instances for each target (e.g. lots of CPUs, lots of containers, lots of virtual machines), which can translate to big mining profits," he said, adding that to boot, monitoring for that sprawling footprint can be difficult to implement, so operations may go undetected for some time.

Past campaigns have included a [cryptojacking worm](#) that spread through misconfigured Docker ports; a brand-new Linux backdoor [called Doki](#) that infested Docker servers and used a blockchain wallet for generating command-and-control (C2) domain names; and in December, [researchers discovered](#) a Monero cryptomining botnet dubbed Xanthe, which has been exploiting incorrectly configured Docker API installations in order to infect Linux systems.

Source: <https://threatpost.com/malicious-docker-cryptomining-images/165120/>



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

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

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

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