
## August 17, 2021

**Challenge yourself with our Safe Surfing quiz!**

This week's stories:


**Ottawa cyber security firm Field Effect detects Windows vulnerabilities giving kernel-level access**

**Hackers claimed to steal data of 100 million T-Mobile customers – server hack confirmed**

**Microsoft discloses new print spooler flaw without patch**

**Dozens of STARTTLS related flaws found affecting popular email clients**

**Cyberattackers embrace CAPTCHAs to hide phishing, malware**

**Experts shed light on new Russian malware-as-a-service written in rust**

**Cryptocurrency heist hacker returns $260m in funds**

**WordPress sites abused in Aggah spear-phishing campaign**

**Ransomware operators exploiting Windows Print Spooler vulnerabilities**

**Microsoft Exchange servers are getting hacked via ProxyShell exploits**

**Malicious Docker images used to mine Monero**

**Wave of native IIS malware hits Windows servers**

**Parcel delivery texts now the most common con-trick**


---

### Ottawa cyber security firm Field Effect detects Windows vulnerabilities giving kernel-level access

Field Effect, an Ottawa-based cyber security company, which provides threat protection services specifically focused on the underserved SMB market, has announced that their security research team has discovered a series of critical zero-day security vulnerabilities which could be exploited to give attackers swift kernel-level privileges in Windows Vista/Server 2008 and all newer releases. These were reported to Microsoft in early May. Microsoft issued patches for the first vulnerability, CVE-2021-34514, in its Patch Tuesday update of July 13, 2021. Patches for the remaining vulnerabilities are scheduled for the fall.

"This patch was the first of a series of vulnerabilities that we disclosed to Microsoft that deal with possible privilege escalations," said Matt Holland, Field Effect's Founder, CEO, and CTO. "They allow an attacker

to upgrade privilege level from basic sandbox level, which is highly protected, to full kernel access. It's the equivalent of going from 0 to 60 easily, and definitely gives the attacker the upper hand. We have updated our Covalence platform to protect against these vulnerabilities, but if an attacker were to find the vulnerabilities in the absence of this kind of protection, it would be very difficult to defend, because the attacker can go from the lowest execution level to the OS kernel so quickly. It is a potential disaster."

*https://channelbuzz.ca/2021/08/ottawa-cyber-security-firm-field-effect-detects-windows-vulnerabilities-giving-kernel-level-access-37340/*

*Click above link to read more.*

Back to top

---

### Hackers claimed to steal data of 100 million T-Mobile customers – server hack confirmed

T-Mobile suffered a data breach that contains the personal details of more than 100 million customers. In an announcement published Monday, T-Mobile confirmed that hackers gained access to the telecom giant's systems.

"We have determined that unauthorized access to some T-Mobile data occurred, however, we have not yet determined that there is any personal customer data involved," T-Mobile wrote in its announcement.

*https://cybersecuritynews.com/t-mobile-data-breach-2/*

*Click above link to read more.*

Back to top

---

### Microsoft discloses new print spooler flaw without patch

Microsoft disclosed a new Windows print spooler vulnerability Wednesday, weeks after the PrintNightmare flaw was first revealed, and this one doesn't have a patch ready.

CVE-2021-36958 is a remote code execution (RCE) vulnerability in Windows print spooler software, which manages a device's printing jobs, that occurs when the software "improperly performs privileged file operations," according to Microsoft's page dedicated to the vulnerability.

*https://searchsecurity.techtarget.com/news/252505269/Microsoft-discloses-new-print-spooler-flaw-without-patch*

*Click above link to read more.*

Back to top

---

### Dozens of STARTTLS related flaws found affecting popular email clients

Security researchers have disclosed as many as 40 different vulnerabilities associated with an opportunistic encryption mechanism in mail clients and servers that could open the door to targeted man-in-the-middle (MitM) attacks, permitting an intruder to forge mailbox content and steal credentials.

The now-patched flaws, identified in various STARTTLS implementations, were detailed by a group of researchers Damian Poddebniak, Fabian Ising, Hanno Böck, and Sebastian Schinzel at the 30th USENIX

Security Symposium. In an Internet-wide scan conducted during the study, 320,000 email servers were found vulnerable to what's called a command injection attack.

*https://thehackernews.com/2021/08/dozens-of-starttls-related-flaws-found.html*

*Click above link to read more.*

Back to top

---

### Cyberattackers embrace CAPTCHAs to hide phishing, malware

Cyberattackers are using Google's reCAPTCHA (aka the "I am not a robot" function) and fake CAPTCHA-like services to obscure various phishing and other campaigns, according to researchers. There are signs however that those evasion efforts may be losing their efficacy.

CAPTCHAs are familiar to most internet users as the challenges that are used to confirm that they're human. The Turing test-ish puzzles usually involve clicking all photos in a grid that contain a certain object, or typing in a word presented as blurred or distorted text.

*https://threatpost.com/cyberattackers-captchas-phishing-malware/168684/*

*Click above link to read more.*

Back to top

---

### Experts shed light on new Russian malware-as-a-service written in rust

A nascent information-stealing malware sold and distributed on underground Russian underground forums has been written in Rust, signalling a new trend where threat actors are increasingly adopting exotic programming languages to bypass security protections, evade analysis, and hamper reverse engineering efforts.

Dubbed "Ficker Stealer," it's notable for being propagated via Trojanized web links and compromised websites, luring in victims to scam landing pages purportedly offering free downloads of legitimate paid services like Spotify Music, YouTube Premium, and other Microsoft Store applications.

*https://thehackernews.com/2021/08/experts-shed-light-on-new-russian.html*

*Click above link to read more.*

Back to top

---

### Cryptocurrency heist hacker returns $260m in funds

The hacker behind one of the largest cryptocurrency heists to date has returned almost half of the $600m (£433m) stolen assets.

On Tuesday, the firm affected, Poly Network wrote a letter on Twitter, asking the individual to get in touch "to work out a solution".

The hacker then posted messages pledging to return funds, claiming to be "not very interested in money".

On Wednesday, Poly Network said it had received $260m back.

*https://www.bbc.com/news/business-58180692*

*Click above link to read more.*

Back to top

---

### WordPress sites abused in Aggah spear-phishing campaign

Threat actors are using compromised WordPress websites to target manufacturers across Asia with a new spear-phishing campaign that delivers the Warzone RAT, a commodity infostealer available widely for purchase on criminal forums, researchers have found.

The threat group Aggah, believed to be affiliated with Pakistan and first identified in March 2019, is delivering the RAT in a campaign aimed at spreading malware to manufacturing companies in Taiwan and South Korea, according to new research from threat detection and response security firm Anomali.

*https://threatpost.com/aggah-wordpress-spearphishing/168657/*

*Click above link to read more.*

Back to top

---

### Ransomware Operators Exploiting Windows Print Spooler Vulnerabilities

The cybersecurity researchers at Cisco Talos have detected that the ransomware group the Vice Society actively exploiting the PrintNightmare vulnerability in the Windows print spooler to relocate its victims over the networks.

However, the experts have stated in one of their reports that PrintNightmare is a collection of vulnerabilities that have CVE-2021-1675, CVE-2021-34527, and CVE-2021-36958 in Windows Print Spooler, Windows drivers, and Windows Point and Print functionality.

*https://cybersecuritynews.com/ransomware-operators-exploiting-windows-print-spooler-vulnerabilities/*

*Click above link to read more.*

Back to top

---

### Microsoft Exchange servers are getting hacked via ProxyShell exploits

Threat actors are actively exploiting Microsoft Exchange servers using the ProxyShell vulnerability to install backdoors for later access.

ProxyShell is the name of an attack that uses three chained Microsoft Exchange vulnerabilities to perform unauthenticated, remote code execution.

*https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-servers-are-getting-hacked-via-proxyshell-exploits/*

*Click above link to read more.*

Back to top

---

### Malicious Docker images used to mine Monero

A recently uncovered cryptomining scheme used malicious Docker images to hijack organizations' computing resources to mine cryptocurrency, according to cybersecurity firm Aqua Security. These images were uploaded to the legitimate Docker Hub repository.

The researchers identified five container images on Docker Hub that could be used as part of a supply chain attack targeting cloud-native environments.

*https://www.bankinfosecurity.com/malicious-docker-images-used-to-mine-monero-a-17283*

*Click above link to read more.*

Back to top

---

### Wave of native IIS malware hits Windows servers

Security researchers warn that multiple groups are compromising Windows web servers and are deploying malware programs that are designed to function as extensions for Internet Information Services (IIS). Such malware was deployed this year by hackers exploiting Microsoft Exchange zero-day vulnerabilities, but a total of 14 groups have been observed using native IIS backdoors and information stealers in recent years.

"IIS malware is a diverse class of threats used for cybercrime, cyberespionage, and SEO fraud – but in all cases, its main purpose is to intercept HTTP requests incoming to the compromised IIS server and affect how the server responds to (some of) these requests," researchers from security vendor ESET said in a recent report.

*https://www.csoonline.com/article/3629130/wave-of-native-iis-malware-hits-windows-servers.html*

*Click above link to read more.*

Back to top

---

### Parcel delivery texts now the most common con-trick

The majority of "smishing" fraud attempts have come through the blitz of parcel delivery texts sent out during the Covid crisis.

Millions of mobile users have received the texts that claim a small payment is needed for a package delivery to be completed.

But the texts are a front for fraudsters attempting to steal personal banking details.
Cybersecurity firm Proofpoint told banks their prevalence was on the rise.

*https://www.bbc.com/news/business-58233743*

*Click above link to read more.*

Back to top

---

**Click unsubscribe to stop receiving the Digest.**

**********



For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca