

June 22, 2021

Challenge yourself with our [Phishing](#) quiz!

[Register for Security Day: TOMORROW](#), June 23, 2021

This week's stories:

 [TransUnion research: Digital fraud on the rise as online banking increases](#)

[CISA: Firewall rules could have blunted SolarWinds malware](#)

[Is an attacker living off your land?](#)

[Ukraine police arrested Clop ransomware gang and disrupted infrastructure](#)

[Ransomware operators' strategies evolve as attacks rise](#)

[Sprawling cyber-espionage campaign linked to Chinese military unit](#)

[Report: Active Directory Certificate Services a big security blindspot on enterprise networks](#)

[‘Oddball’ malware blocks access to pirated software](#)

[NHS Test and Trace strengthens cyber defences](#)

[Attackers find new way to exploit Google Docs for phishing](#)

TransUnion research: Digital fraud on the rise as online banking increases

According to credit reporting agency TransUnion, as more consumers do their banking and financial transactions online, fraudsters are also ramping up their efforts.

Comparing the last four months of 2020 to the first four months of 2021, the company said it found the percentage of suspected digital fraud attempts in financial services coming from Canada increased 218%. Globally, the rate of financial services fraud attempts increased 149%.

<https://www.canadiansecuritymag.com/transunion-research-digital-fraud-on-the-rise-as-online-banking-increases/>

Click above link to read more.

[Back to top](#)

CISA: Firewall rules could have blunted SolarWinds malware

Federal agencies could have prevented follow-on attacks after the SolarWinds supply chain attack by using recommended firewall configurations, but this step isn't always feasible, the Cybersecurity Infrastructure and Security Agency says.

That advice came in a June 3 letter written by CISA acting Director Brandon Wales. Wales was responding to questions posed by Sen. Ron Wyden, D-Ore., about the SolarWinds attack. Wyden had questioned CISA about the cybersecurity readiness of federal agencies, Reuters reported on Monday.

<https://www.bankinfosecurity.com/cisa-firewall-rules-could-have-blunted-solarwinds-malware-a-16919>

Click above link to read more.

[Back to top](#)

Is an attacker living off your land?

Malware – and all of its various forms, including ransomware – has grown increasingly stealthy and sophisticated in recent years. Also on the rise: Its ability to fly under cybersecurity software's radar.

One of the primary reasons detecting and stamping out malware is so difficult is the rise of an attack method called living off the land (LotL). Despite conjuring up idyllic images of urban farming or sustainability, the term refers to a group of techniques that typically execute in shell code or scripts running in memory.

<https://www.darkreading.com/edge/theedge/is-an-attacker-living-off-your-land/b/d-id/1341303>

Click above link to read more.

[Back to top](#)

Ukraine police arrested Clop ransomware gang and disrupted infrastructure

Members of the Clop ransomware gang arrested by the Ukrainian police in conjunction with Interpol and law enforcement from the US and South Korea.

With the help of the malicious program "Clop", the defendants encrypted the data on the media of companies in the Republic of Korea and the United States. Later on, they demanded money to restore access.

<https://cybersecuritynews.com/clop-ransomware-gang/>

Click above link to read more.

[Back to top](#)

Ransomware operators' strategies evolve as attacks rise

Security researchers find ransomware operators rely less on email and more on criminal groups for initial access into target networks.

Corporate email inboxes remain a valuable target for many cybercriminals, but ransomware operators are finding new avenues into enterprise networks as defensive tools improve, new research shows.

Ransomware attackers have begun to leverage criminal organizations, mostly banking Trojan distributors, for malware deployment.

<https://www.darkreading.com/attacks-breaches/ransomware-operators-strategies-evolve-as-attacks-rise/d/d-id/1341327>

Click above link to read more.

[Back to top](#)

Sprawling cyber-espionage campaign linked to Chinese military unit

Cybersecurity experts have uncovered evidence that interconnects several multi-year and sprawling cyber-espionage campaigns to a Chinese military unit operating out of the city of Ürümqi in China's western province of Xinjiang.

According to a report released today by Recorded Future's Insikt Group, the People's Liberation Army (PLA) Unit 69010 is believed to have been behind a series of cyber-espionage campaigns dating back to 2014 that have focused on gathering military intelligence from neighboring countries.

https://therecord.media/sprawling-cyber-espionage-campaign-linked-to-chinese-military-unit/?web_view=true

Click above link to read more.

[Back to top](#)

Report: Active Directory Certificate Services a big security blindspot on enterprise networks

Microsoft's Active Directory PKI component commonly have configuration mistakes that allow attackers to gain account and domain-level privileges.

As the core of Windows enterprise networks, Active Directory, the service that handles user and computer authentication and authorization, has been well studied and probed by security researchers for decades. Its public key infrastructure (PKI) component, however, has not received the same level of scrutiny and, according to a team of researchers, deployments are rife with serious configuration mistakes that can lead to account and domain-level privilege escalation and compromise.

<https://www.csoonline.com/article/3622352/report-active-directory-certificate-services-a-big-security-blindspot-on-enterprise-networks.html>

Click above link to read more.

[Back to top](#)

‘Oddball’ malware blocks access to pirated software

Rather than steal credentials or hold data for ransom, a recent campaign observed by Sophos prevents people from visiting sites that offer illegal downloads.

The objective of most malware is some kind of gain — financial or otherwise — for the attackers who use it. However, researchers recently observed a unique malware with a single intent: Blocking the infected computers from visiting websites dedicated to software piracy.

<https://threatpost.com/oddball-malware-blocks-pirated-software/167060/>

Click above link to read more.

[Back to top](#)

NHS Test and Trace strengthens cyber defences

NHS Test and Trace is working with British cybersecurity company Risk Ledger to proactively manage cybersecurity risks in their supply chain.

The UK government-funded service, which was established to track and help prevent the spread of the COVID-19 virus in England, will utilise Risk Ledger's secure 'social network' platform, which allows organisations to connect and share risk data securely.

<https://www.healthcareitnews.com/news/emea/nhs-test-and-trace-strengthens-cyber-defences>

Click above link to read more.

[Back to top](#)

Attackers find new way to exploit Google Docs for phishing

Tactic continues recent trend by attackers to use trusted cloud services to send and host malicious content.

Researchers spotted what they describe as a new method that attackers appear to be using to lure victims to malicious phishing websites via Google Docs.

The attack chain begins with the threat actor sending potential victims an email—on a topic of likely interest or relevance to the victim—with a link to a document on Google Docs. Users who follow the link are directed to a Google Docs page with what appears to be a downloadable document, according to researchers at Avanan.

<https://www.darkreading.com/vulnerabilities---threats/attackers-find-new-way-to-exploit-google-docs-for-phishing-/d/id/1341342>

Click above link to read more.

[Back to top](#)

Click [Unsubscribe](#) to stop receiving the Digest.

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

