



October 6th, 2020

Challenge yourself during Cyber Security Awareness Month

Try our October - 'Cyber Security Awareness Month' Quiz

This week's stories:

- [MapleSEC: The ransomware attack that turned into a horror story](#) 
- [Happy Valley-Goose Bay's policy for body cameras being reviewed by privacy](#) 
- [ZeroLogon Attacks Against Microsoft DCs Snowball in a Week](#)
- [State-Sponsored Hacking Groups Increasingly Use Cloud & Open Source Infrastructure](#)
- [Federal IoT Guidelines Move Closer to Becoming Law](#)
- [SilentFade malware stole Facebook credentials, \\$4 million in ad fraud](#)
- [A China-Linked Group Repurposed Hacking Team's Stealthy Spyware](#)
- [To hunt hackers, FBI works more closely with spy agencies](#)
- [Ransomware Victims That Pay Up Could Incur Steep Fines from Uncle Sam](#)
- [U.K. Found 'Critical' Weakness in Huawei Equipment](#)
- [Blackbaud: Bank details and passwords at risk in giant charities hack](#)

MapleSEC: The ransomware attack that turned into a horror story

<https://www.itworldcanada.com/article/maplesec-the-ransomware-attack-that-turned-into-a-horror-story/436726>

If you want to hear cyberattack horror stories, ask a penetration tester.

But you might have trouble beating the one pen tester Terry Cutler of Montreal's Cyology Labs told Monday during the MapleSec online conference hosted by *IT World Canada*.

It started with a plea for help he received on a Sunday night from an unnamed Canadian laboratory with offices across the country. It had been hit two days earlier by a ransomware attack.

[Click link above to read more](#)

Happy Valley-Goose Bay's policy for body cameras being reviewed by privacy commissioner

<https://www.cbc.ca/news/canada/newfoundland-labrador/happy-valley-goose-bay-body-cams-privacy-1.5750738>

The Town of Happy Valley-Goose Bay has outfitted its municipal enforcement and animal control officers with body cameras, while the province's privacy commissioner is reviewing the town's policies to ensure they are in line with privacy laws.

Council first made the move toward body cams for its officers back in February, with first use set for March 4, but backed off from that plan.

[Click link above to read more](#)

Zerologon Attacks Against Microsoft DCs Snowball in a Week

<https://threatpost.com/zerologon-attacks-microsoft-dcs-snowball/159656/>

The attempted compromises, which could allow full control over Active Directory identity services, are flying thick and fast just a week after active exploits of CVE-2020-1472 were first flagged.

A spike in exploitation attempts against the Microsoft vulnerability CVE-2020-1472, known as the Zerologon bug, continues to plague businesses.

[Click link above to read more](#)

State-Sponsored Hacking Groups Increasingly Use Cloud & Open Source Infrastructure

<https://www.darkreading.com/threat-intelligence/state-sponsored-hacking-groups-increasingly-use-cloud-and-open-source-infrastructure/d/d-id/1339030>

Espionage groups increasingly use cloud-based services and open source tools to create their infrastructure for gathering data and cyberattacks, attempting to hide their activities in the massive quantity of services and resources used by legitimate organizations.

Last week, Microsoft suspended 18 Azure Active Directory "applications" that the company identified as a component of a Chinese espionage group's command-and-control channel. Dubbed GADOLINIUM by Microsoft, the cyberattack group has adopted a combination of cloud infrastructure, which can be quickly reconstituted in the event of a takedown, and open source tools, which can help attackers' actions blend into more legitimate activity.

[Click link above to read more](#)

Federal IoT Guidelines Move Closer to Becoming Law

<https://www.inforisktoday.com/federal-iot-guidelines-move-closer-to-becoming-law-a-15085>

The House passed the Internet of Things Cybersecurity Improvement Act of 2020 on Sept. 14, and it now awaits a vote by the Senate. Whether that will happen in a tumultuous election year remains to be seen. But chances are better than ever for Senate support for the legislation, which has been in the works for three years, because the bill has been rewritten to make it less prescriptive, allowing for changes but without requiring Congress to pass new legislation.

[Click link above to read more](#)

SilentFade malware stole Facebook credentials, \$4 million in ad fraud

<https://www.hackread.com/silentfade-malware-facebook-credentials-ad-fraud/>

Facebook's security experts discovered a sophisticated Chinese-sponsored malware campaign stealing millions of dollars from users through SilentFade malware in 2018.

Facebook's security team successfully shut down the malicious scheme and shared the scam's full details at last week's Virus Bulletin 2020 security conference.

[*Click link above to read more*](#)

A China-Linked Group Repurposed Hacking Team's Stealthy Spyware

<https://www.wired.com/story/hacking-team-uefi-tool-spyware/>

When a hacking organization's secret tools are stolen and dumped online for anyone to pick up and repurpose, the consequences can roil the globe. Now one new discovery shows how long those effects can persist. Five years after the notorious spy contractor Hacking Team had its code leaked online, a customized version of one of its stealthiest spyware samples has shown up in the hands of possibly Chinese-speaking hackers.

[*Click link above to read more*](#)

To hunt hackers, FBI works more closely with spy agencies

<https://www.infosecurity-magazine.com/news/ebay-execs-to-plead-guilty-to/>

Four former eBay executives accused of cyber-stalking and intimidating a Massachusetts couple are to admit their guilt before a court next month.

The married couple, an editor and a publisher residing in Natick, were targeted with a series of terrifying deliveries after they criticized eBay in an online newsletter.

Horrific parcels sent to the couple included a bloody pig mask, live spiders and cockroaches, a book on surviving the death of a spouse, and a wreath of funeral flowers. In addition, pornographic magazines addressed to the husband were received by one of the couple's neighbors.

[*Click link above to read more*](#)

Ransomware Victims That Pay Up Could Incur Steep Fines from Uncle Sam

<https://krebsonsecurity.com/2020/10/ransomware-victims-that-pay-up-could-incur-steep-fines-from-uncle-sam/comment-page-1/>

In its advisory (PDF), the Treasury's Office of Foreign Assets Control (OFAC) said "companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations."

[*Click link above to read more*](#)

U.K. Found 'Critical' Weakness in Huawei Equipment

<https://www.bloomberg.com/news/articles/2020-10-01/u-k-found-critical-weakness-in-huawei-equipment-last-year>

British intelligence forced Huawei Technologies Co. to fix flaws in its products that could have put the security of the country's networks at risk, a government agency said.

"Critical, user-facing vulnerabilities" were found in the Chinese supplier's fixed-broadband products caused by poor code quality and an old operating system, the Huawei Cyber Security Evaluation Centre Oversight Board said in a report. "U.K. operators needed to take extraordinary action to mitigate the risk."

[Click link above to read more](#)

Blackbaud: Bank details and passwords at risk in giant charities hack

<https://www.bbc.com/news/technology-54370568>

Bank account information and users' passwords are among details feared stolen by hackers in a security breach at a service used to raise donations from millions of people.

Many UK universities and charities, as well as hundreds of other organisations worldwide, use the software involved. Its developer Blackbaud made the admission in a regulatory filing.

The firm previously said the theft had been limited to other personal data - but not payment details.

It added it was contacting affected clients. They, in turn, will need to send follow-up alerts to at least some of the donors they had already contacted about the incident.

[Click link above to read more](#)

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.

