23 July 2018

THREAT INTELLIGENCE
SUMMARY - TISUM

Address: 7506 Holley Circle, Panama City, Florida 32408

Phone: +1 850.387.2888

https://www.janyx.com

Threat Intelligence Summary

Janyx, Inc

TISUM 180723

Contents

Disclaimer

Data Breaches

LabCorp Potential Breach

On 16 July 2018 Laboratory Corporation of American Holdings filed a Form 8-K with the Security Exchange Commission informing shareholders that an investigation into suspicious activity on the LabCorp information network had been initiated. LabCorp recently released a press release[1] advising customers and shareholders that the suspicious activity had been identified as a ransomware infection and remediation efforts were still ongoing. Additionally, LabCorp feels that currently there are no indications that data has been compromised.

85% of cyber incidents are attributed to human error.

ComplyRight Sensitive Data Breach

In May 2018, ComplyRight detected suspicious activity on their web-based platform. On 18 July 2018, ComplyRight announced[2] the details of what been compromised in the breach. It has been determined that sensitive personally identifiable information such as names, social security numbers, emails, addresses, and phone numbers had been compromised. Although establishing unauthorized access to the data, current evidence cannot confirm or deny as to whether data had been exfiltrated for the compromised system(s).

The intrusion vector has not been publicly disclosed or whether the intrusion vector has been identified. The press statement by ComplyRight does allude to the web platform being the limit of the compromise and has not suggested that any further breach of the internal information network.

More Healthcare Breaches and Leaks

In addition to the LabCorp compromise, two other healthcare providers were breached. Nashville Metro Public Health was reported[3] to have compromised the data of HIV/AIDS patients due to a misconfiguration of permissions to access the data. The data was accessible to any employee of the agency. The data contained PII such as names, social security numbers, contact information, as well as protected health information (PHI) including lab results, use of illicit narcotics, sexual orientation and gender status. The data contained information on patients dating back to 1983.

On 13 July 2018, the Rocky Mountain Health Care Services (RMHCS) issued a press release[4] indicating that PII and PHI had been compromised due to a stolen laptop. The press release stated that the data had been stored locally on the computer potentially allowing the perpetrator to access the data. As with the other breaches and leaks, names, addresses, social security numbers, and other health related information had been potentially compromised.

Latest Attacks

II

China Targets IoT Devices During Finland Summit

During the United States / Russia summit in Helsinki, Finland an increased number of attacks against IoT devices were observed[5]. The attacks that originated from China focused on the targeting of TCP port 22 (SSH) and port 445 (SMB). During the United States / North Korea summit, similar behavior was observed with Russia being the top origin of attacks. Russian attacks primarily targeted TCP port 5060 (SIP). Multiple other TCP and UDP ports were also targeted but not to the extent as the previously mentioned ports.

Hackers Heist $1 Million from Russian Bank

A Russian bank, PIR Bank, LLC, was the victim of a cyber attack starting in late May. The heist is believed to have been valued at over $920K. The vulnerability was reportedly[6] an outdated router located in a regional branch that was exploited allowing the attackers to gain access to the bank's local network. The investigating firm, Group-IB, has attributed the attack to a hacking group known as MoneyTaker. The funds stolen from the bank were transferred to cards of 17 of the largest banks.

Sextortion Phishing Scam

A recent phishing scam has been reported[7] that is perpetrated in a manner that makes it effective against unwitting victims. The phishing email contains a password that has been associated with the victim's email from a previously confirmed compromise. Because the victim knows this password to be real or used in the past, a sense of legitimacy is conveyed. The phishing email threatens to extort the victim by stating they have been monitored on pornographic websites. The perpetrator demands a sum in bitcoin or other alternative cryptocurrency on a threat of disclosure of the pornographic activity.

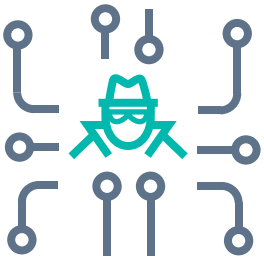
Malware Trends

III

Week In Review

The most common malware seen in the past week is the Win32/Zegost backdoor and trojan virus. The Win32/Zegost connects to command and control (C2) domains to exfiltrate data from the infected host. Because the Win32/Zegost has a backdoor incorporated into the malware, the intruder can also remotely connect to the infected host. The malware also makes modifications to the Windows Registry in order to configure the malware be autorun when the infected host is booted.

Like the Win32/Zegost malware, backdoors and trojans made up the bulk of malware tracked in the wild during the past week. File infectors and worm viruses made up the smallest portion of malware observed. Malware such as ransomware, password stealers, and crypto-miners made up about 30% of malware found. Exploit kits are seeing more activity to target legacy systems with older vulnerabilities. Exploit kits seen active were KaiXin, Sundown, Rig, and Sinowal. The United States, China, and Russia are still the top countries for the location of malicious domains and attack origins.



Emotet Malware

A recently discovered malware is disrupting commercial, government and personal banking[8]. The Emotet malware primarily operates as a downloader or dropper. A dropper is a malware that will download other malware or viruses from another source and attempt to install the new malware on the infected host. Emotet is polymorphic which allows the malware to avoid static signature-based detection. Because of the recent developments of Emotet, only a few anti-virus engines are capable of detecting the malware. The primary delivery vector of the malware is through phishing emails. The best defense against this threat is ensuring the awareness of phishing emails, the use of host intrusion detection systems (HIDS), updating anti-virus software with the latest signatures.

Overall Analysis

The threats encountered over the past week covered the entire spectrum of information security threats. Threats observed included human error, social engineering, natural disasters, cyber espionage, and hacking. The outliers in the activity seen were the number of healthcare organizations that suffered breaches, leaks, and social engineering campaigns. Almost a dozen health care organizations reported data compromise.

Healthcare Breaches. The data breaches reported recently demonstrate both human error and proactive monitoring of information networks. The LabCorp incident, while not yet determined to be strictly a ransomware attack, was classified as a data breach because of the recent trend of healthcare organizations falling victim to compromise. The health care industry initially appears to be targeted with social engineering campaigns designed to obtain both PII and PHI. Five disclosed health care organizations fell victim to email phishing campaigns with another reporting at least one hacked email account.

Intrusions. The ComplyRight intrusion vector has not been disclosed. Any attempt to identify the vector used in the attack would be speculation. The more common vectors seen in web-based intrusions are vulnerabilities in the host configuration, web server software, or the web-based applications in use on the server. It could be possible that an unpatched vulnerability was exploited just as seen in the PIR Bank intrusion. The attacks seen in Finland were more brute-force oriented than unpatched vulnerabilities. The focus of the attacks in Finland are indicative of automated brute-force attacks as the targets were TCP ports used by common web-based applications such as SSH, MYSQL, RDP, and SIP. The vulnerabilities in those cases would be legacy systems vulnerable to SMB exploits and weak passwords of administrative users for those applications.

Social Engineering. The conduct of phishing campaigns demonstrates that social engineering is still one of the primary threats to information and cyber security. Unlike the health care data breaches, the sextortion campaign conducted in the past week was primarily a financial cyber crime operation. The action which made the emails so compelling was the use of passwords and emails known to the victims. Emails and passwords are gathered from various breaches into a collective list, known as credential stuffing. These valid credentials are then used in an attempt to take over accounts of other services which use the same email/password combination. The credential stuffing is most likely the source of information used against the victims of the sextortion campaign.

Bibliography

1 "LabCorp." LabCorp | The World's Leading Health Care Diagnostics Company. July 23, 2018. https://www.labcorp.com/content/labcorp-it-security-information.

2 "ComplyRight Data Security Incident Notice." ComplyRight Solutions. July 18, 2018. https://www.complyright.com/data-security-notice.

3 Kelman, Brett. "Identities of Thousands of Tennesseans with HIV Made Vulnerable by Government Error." The Tennessean. July 11, 2018. https://www.tennessean.com

4 "Data Security Incident." RMHCS. July 13, 2018. Accessed July 23, 2018. https://www.rmhcare.org/data-security-incident/.

5 Boddy, Sara, and Justin Shattuck. "Cyber Attacks Spike in Finland Before Trump-Putin Meeting." F5 Networks. July 19, 2018. https://www.f5.com/

6 Leyden, John. "Cybercrooks Slurp Nearly $1m from Russian Bank after Pwning Router at Regional Branch." The Register® - Biting the Hand That Feeds IT. July 20, 2018. https://www.theregister.co.uk/

7 Crowe, Jonathan. "New Sextortion Scam Flaunts Real Passwords, Rakes in $50,000 in a Week." Barkly Endpoint Security Blog. July 2018. https://blog.barkly.com/new-sextortion-scam-real-passwords-fake-threat.

8 "Alert (TA18-201A) Emotet Malware." Virus Basics | US-CERT. July 20, 2018. https://www.us-cert.gov/ncas/alerts/TA18-201A.

JANYX
INNOVATIVE CYBER SECURITY SOLUTIONS

Prepared By:
David Mans
Cyber Security and Computer Forensics Analyst
david.mans@janyx.com
850.387.2888 x 1031

Address: 7506 Holley Circle, Panama City, Florida 32408
Phone: +1 850.387.2888
https://www.janyx.com

JANYX
INNOVATIVE CYBER SECURITY SOLUTIONS

Phone: +1 850.387.2888

Address: 7506 Holley Circle, Panama City, Florida 32408

https://www.janyx.com