telelink
BUSINESS SERVICES

Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

July 2019

telelink BUSINESS SERVICES

This security bulletin is powered by Telelink's

Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

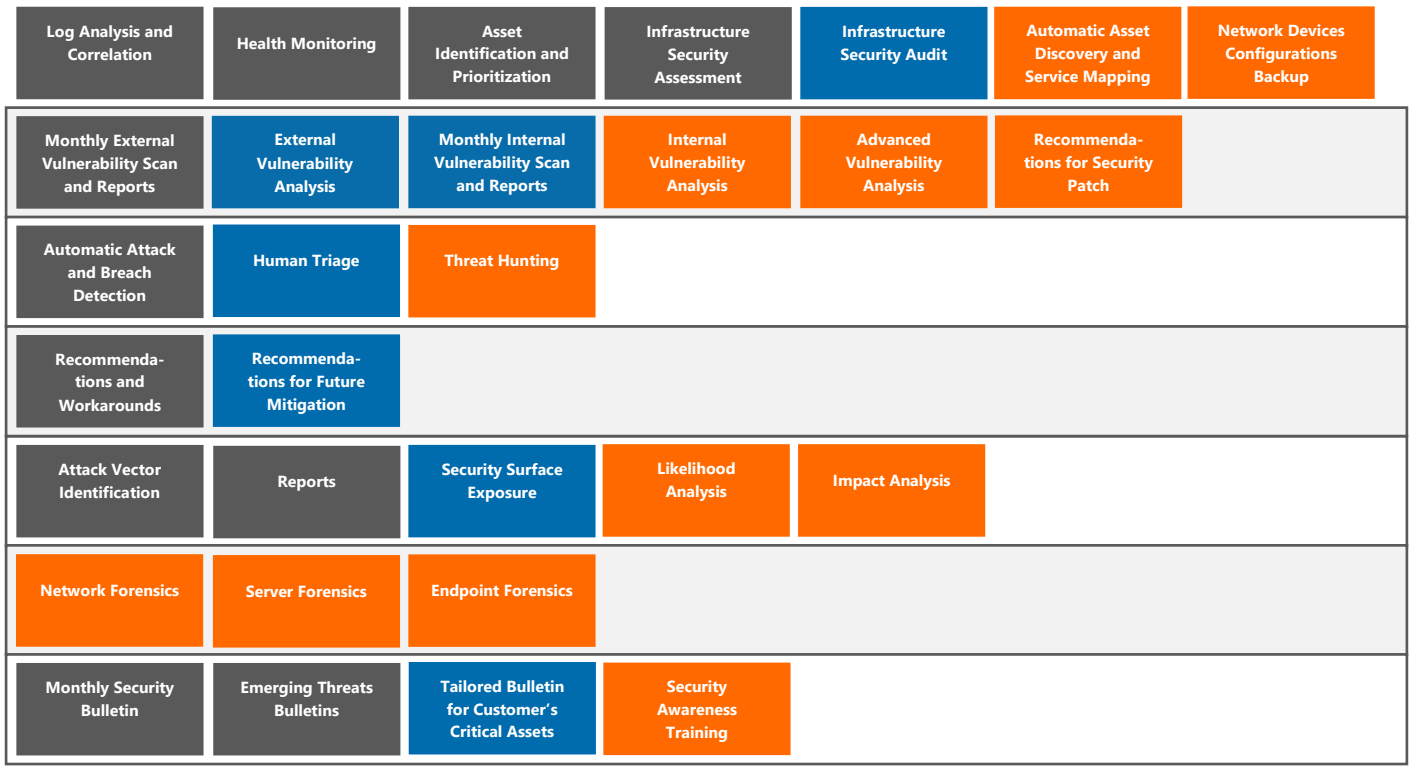
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!



What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state of the art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Executive summary

1. 440 Milion users of Android have installed mobile ad plugin, found in hundreds of Google Play apps, that uses well-honed techniques from malware development to hide itself. The plugin is used to deliver obnoxious advertising plugin, which ultimately can render phones almost unusable.→
2. The Iranian MuddyWater cyber-espionage group added new attack vectors - decoy macro-powered Microsoft Word documents that drop payloads via compromised servers and new documents designed to leverage CVE-2017-0199 →
3. The hack of the American Medical Collection Agency (AMCA), a third-party bill collection vendor, continues to expand, now impacting 20.1 million patients with exposed information that includes personally identifiable information such as names, addresses and dates of birth, but also payment data. The breach involved three clinical laboratories offering blood tests that relied on AMCA to process a portion of their consumer billing. The culprit in the breach appears to be an insecure web payments page maintained by AMCA that consumers could use to pay their bills. →
4. Ghanaian Muftau Adamu was sentenced on June 7, 2019 to 51 months in prison by US court for stealing more than $10 million through romance scams and business email compromise (BEC) fraud schemes aided by four other co-conspirators, between 2014 and 2018. See inside for detailed explanation of their modus operandi. →
5. K-12 schools are under increasing pressure to protect the personal information of their students, along with the physical safety of the students themselves as they are popular targets for cybercriminals looking to steal data and exploit resources. So, in addition to performance issues, extra care must be taken to protect connected devices against viruses, data breaches, and malware. →
6. A denial of service flaw found in the way recent Linux kernels handle TCP networking can be exploited by remote attackers to trigger a kernel panic in vulnerable systems. One of the vulnerabilities got a 7.5 CVSS3 base score. Patches are already available as detailed in Netflix's NFLX-2019-001 security advisory, with mitigation measures also being available for machines where patching is not an immediate or easy option. →
7. An analysis of decade of data breaches shows a bleak picture with billions of records exposed in this type of incidents and cumulative financial damages of more than $1.6 trillion. Data collected from public sources reveal that since 2008 there were close to 9,700 breach events in the U.S., involving more than 10.7 billion records, with an average cost calculated in 2018 at $148 per record. →
8. Sensitive personal information of roughly 2.9 million Desjardins Group (largest association of credit unions in North America) members was leaked after an employee disclosed it to people outside the organization without authorization. →
9. Millions of PCs made by Dell and other OEMs are vulnerable to a flaw ((CVE-2019-12280) stemming from a component in pre-installed SupportAssist software (used to check the health of system hardware and software and as such requires high permissions). The flaw could enable a remote attacker to completely takeover affected devices and is classified as high-severity vulnerability. Patch is available. →

10. Over 58% of the phishing websites detected in the first quarter of the year used digital certificates to encrypt the connections from the visitor as a way to prevents third parties and security systems from viewing the data that's exchanged. This is 12% jump over last year and is continuing trend that cybercriminals use to increase efficiency and prevent security system from stopping the malicious traffic. →
11. Multiple malicious campaigns observed in April concealed LokiBot and Nanocore malware inside ISO image files small enough to fit into an email attachment. This is a way to deliver malware to user inbox, as some security solutions tend to whitelist ISO files for performance reasons. →
12. Hackers launching ransomware attacks against City of Lake and Riviera Beach city in Florida locked earnings in excess of $1 million this month as administrators of the two cities found no other way to recover files on affected systems. Following a ransomware attack - dubbed "Triple Threat". Both incidents occurred because an employee ushered in the malware by opening a malicious email and backup policies and systems, if they were available, did not work properly. →
13. Cisco released today patches for web-management console of its Data Center Network Manager (DCNM) software fixing critical vulnerabilities that allow a remote attacker to upload files and execute actions with root privileges. The updates cover four security bugs, two of them standing out through a close-to-maximum severity score of 9.8 out of 10. Addressed vulnerabilities are CVE-2019-1619, CVE-2019-1620, CVE-2019-1621, CVE-2019-1622. →
14. New ATM malware sample, capable of cashing out ATMs, written in Java that was uploaded to a multiscanner service from Mexico and later from Colombia. Malwared was called ATMJaDi and uses the victim bank's ATM software Java proprietary classes: meaning the malware will only work on a small subset of ATMs. →

Contents

1. 440 Million Android Users Plagued By Extremely Obnoxious Pop-Ups

The mobile ad plugin, found in hundreds of Google Play apps, uses well-honed techniques from malware development to hide itself.

Over 440 million Android phones have been exposed to an obnoxious advertising plugin hidden within hundreds of popular applications available via Google Play, which ultimately can render phones almost unusable.

Lookout Research discovered the plugin being bundled with 238 unique applications that have racked up millions of downloads between them – all from one company in China, CooTek. Dubbed BeiTaPlugin, the ad module forcibly displays ads on the user's lock screen, triggers video and audio advertisements (even while the phone is asleep) and displays out-of-app ads in other areas too.

"Users have reported being unable to answer calls or interact with other apps, due to the persistent and pervasive nature of the ads displayed," Lookout said in a posting on Tuesday.

Developers of free mobile apps turn to advertising plugins to monetize their wares. These automatically fetch ads at specified times to display, usually within the context of the application itself. For instance, when a player completes a level in a mobile game, he usually has to suffer through a 30-second ad before being able to go onto the next challenge.

However, out-of-app ads skirt the line between legitimate business modeling and obtrusive scamminess by pushing pop-up ads to users when they're doing other things. The offending app could push an ad to the notification area of the phone, or present a pop-up anywhere, anytime – and the unfortunate part is that the user wouldn't know which app is the one being obnoxious.

BeiTaPlugin takes this dodgy practice to an entirely new level, according to Lookout, by employing obfuscation techniques normally reserved for standard malware in order to hide from utilities that block or detect out-of-app ad plugins.

For instance, it takes a little sleep before swinging into action. "These ads do not immediately bombard the user once the offending application is installed, but become visible at least 24 hours after the application is launched," the researchers said. "For example, obtrusive ads did not present themselves until two weeks after the application 'Smart Scan' had been launched on a Lookout test device."

The BeiTaPlugin also hides its true nature by appending fake file names and suffixes to its components. It names itself "icon-icomoon-gemini.renc" in the system files – purporting to be a legitimate application called Icomoon, which is an application that provides vector icon packs for designer and developer use. One of those icon packs is named Gemini.

"Malware authors commonly employ this technique of renaming executable files to other file types (pdf, jpg, txt) to hide malicious assets in plain sight," researchers said. "In both cases, the .rec or .renc filetype suffix is intentionally misleading; the file is actually .dex (Dalvik Executable) file type that contains executable code rather than an innocuous .renc file."

The package is also encrypted, and the AES encryption key is obfuscated through a series of connected methods and finally called for use by a package named "Hades SDK."

"Increased encryption and obfuscation techniques are applied to hide the plugin's existence," explained Lookout researchers. "All strings related to plugin activity are XOR-encrypted and Base64-encoded, courtesy of a third-party library called StringFog. Each class that facilitates the loading of the plugin is encrypted with its own separate key."

BeiTaPlugin was bundled a popular keyboard app, TouchPal, as well as numerous add-ons to the TouchPal keyboard, and several popular health and fitness apps, according to Lookout. Lookout reported the malicious functionality to Google, and the adware has now been removed from all the affected apps on the Play store – although users with the apps already installed are still likely affected.

Google Play and other app stores are cracking down on the use of out-of-app advertising, so it's likely that the BeiTaPlugin saga is a sign of things to come, researchers noted.

"This BeiTaPlugin family provides insight into future development of mobile adware," Lookout said. "As official app stores continue to increase restrictions on out-of-app advertisements, we are likely to see other developers employ similar techniques to avoid detection."

Source: https://threatpost.com/android-completely-obnoxious-pop-ups/145390/

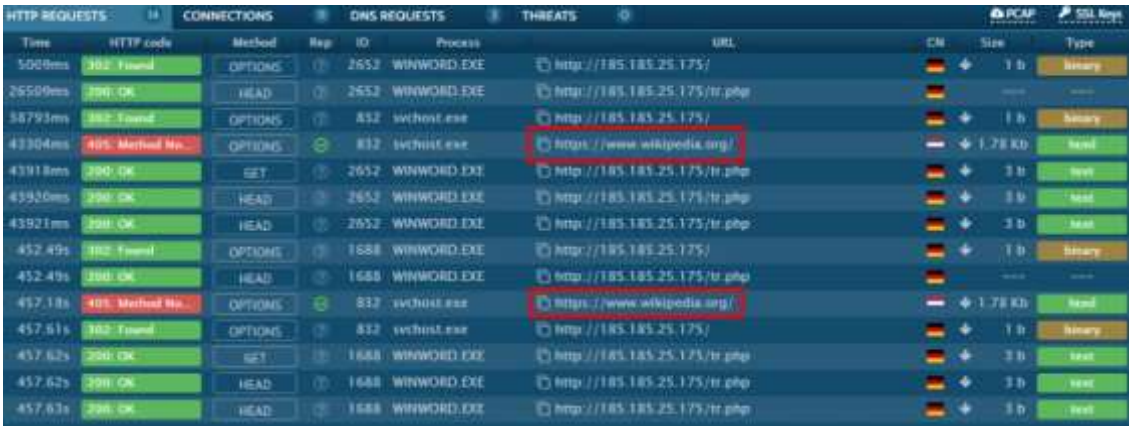
2. The MuddyWater APT Group Adds New Tools to Their Arsenal

The Iranian MuddyWater cyber-espionage group added new attack vectors to use as part of hacking campaigns targeting telecommunication and governmental organizations according to an analysis from the Clearsky Security threat intelligence outfit.

This happened despite the advanced persistent threat (APT) group — or government-backed hacking group — having screenshots of their server backends and one of their command-and-control (C2) server's codebase leaked via a Telegram channel during early-May.

MuddyWatter actors have supplemented their tactics, techniques, and procedures (TTPs) with new decoy macro-powered Microsoft Word documents that drop payloads via compromised servers and new documents designed to leverage the tried-and-true CVE-2017-0199 also known as Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API.

The documents which deliver VBA macros to the targets' computers will download a second stage malware payload camouflaged as JPG files from hacked servers located in the same countries as the potential victims.



Wikipedia redirection

The ones designed to exploit CVE-2017-0199 "were identified by only three antivirus engines. This is in stark comparison to a previous attack we reported on, in which the documents were identified 32 times," says the Clearsky Security report.

Once the victim's computer gets compromised, the malware tries to phone home to the attackers' C2 servers and, if the attempt fails, the victim gets redirected to Wikipedia.

To exploit the CVE-2017-0199 flaw, MuddyWatter uses two types of decoy documents, with the first one making use of error messages while the second will exploit the vulnerability right after they are opened by the victims.

The Clearsky Security researchers also found that some of the decoy files utilized by the Iranian APT were using both attack vectors.

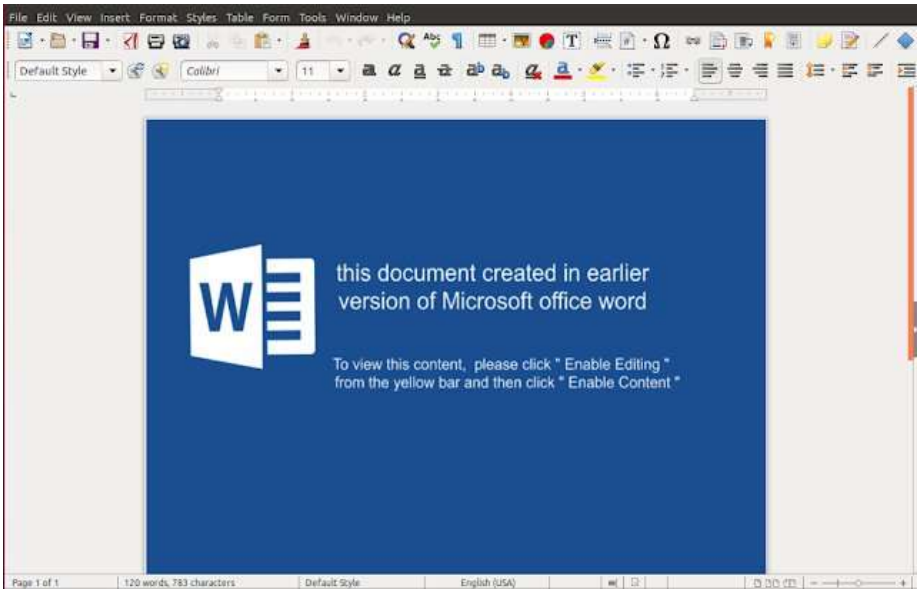
The first exploits the Microsoft Office/WordPad RCE vulnerability, and subsequently downloads the first and second stage payloads from actor-controlled C2 servers and drops them on the targets' machines.

MuddyWatter decoy documents

MuddyWater (also known as TEMP.Zagros and SeedWorm) was first observed in 2017 and is known by experts to mainly target Midle Eastern entities.

Although quite new on the scene, this APT group is very active given that it made 131 victims in 30 organizations from late-September to mid-November 2018 according to a Symantec report from December 2018.

MuddyWater was also observed while diversifying their attacks by targeting government and defense entities in Central and Southwest Asia, as well as numerous public and privately-held organizations from Europe, Asia, and North America.



Trojanized BlackWater document (Image: Cisco Talos)

As discovered by Cisco Talos during May, the MuddyWater threat group updated their TTPs to incorporate several new anti-detection techniques designed to provide remote access to infiltrated systems while evading detection as part of a campaign dubbed BlackWater.

During the BlackWater campaign, the APT group made extra efforts to avoid detection after compromising targets by attempting to avoid Yara rules and host-based signatures using modified tools, replacing variable names used by their malicious implants but also making sure that the overall functionality and structure remained untouched.

Source: *https://www.bleepingcomputer.com/news/security/the-muddywater-apt-group-adds-new-tools-to-their-arsenal/*

3. AMCA Healthcare Hack Widens Again, Reaching 20.1M Victims

OPKO subsidiary BioReference joins Quest and LabCorp in the supply-chain incident.

The hack of the American Medical Collection Agency (AMCA), a third-party bill collection vendor, continues to expand, now impacting 20.1 million patients across three laboratory services providers.

In the wake of revelations that the personal data of 12 million patients from Quest Diagnostics had been potentially compromised by an infiltration of AMCA systems, another 7.7 million patients from LabCorp were shown on Wednesday to be impacted. And, 400,000 victims from OPKO Health have been now been added to the tally as of Thursday.

The exposed information includes personally identifiable information such as names, addresses and dates of birth, but also payment data. All three companies are clinical laboratories offering blood tests and the like, and all three relied on AMCA to process a portion of their consumer billing.

In a filing with U.S. Securities and Exchange Commission (SEC), AMCA told OPKO that an unauthorized party accessed the data of around 422,600 patients between August 1 and March 30, 2019 (the same dates affecting the other two providers). The information was provided by BioReference, an OPKO subsidiary, and "may have included patient name, date of birth, address, phone, date of service, provider and balance information. In addition, the affected AMCA system also included credit card information, bank account information (but no passwords or security questions) and email addresses that were provided by the consumer to AMCA….no Social Security Numbers were compromised…and no laboratory results or diagnostic information."

AMCA also said that it will send breach notifications to "6,600 patients for whom BioReference performed laboratory testing" whose payment card information was exposed.

The culprit in the breach appears to be an insecure web payments page maintained by AMCA that consumers could use to pay their bills – it has been taken down, according to the filing. AMCA also said that it has hired a firm to help it improve its security posture overall.

That's probably a good thing, given that Mounir Hahad, head of Juniper Threat Labs at Juniper Networks, noticed that the payment page isn't the only page lacking security on the site.

"It is telling that AMCA's main website does not enforce encryption like most websites do, and when you manually switch to HTTPS to try to secure the connection, it presents you with the wrong certificate for another web site called retrievalmasterscreditorsbureau.com, which also happens to have expired a year ago," he said, via email.

While lab results don't seem to be part of the mix of exposed information according to the SEC filing, Quest did say in its notice that "AMCA's affected system included information provided by Quest to help patients understand what they were being charged for, and to allow patients to submit an insurance claim when appropriate" – which could include personal health data.

Medical-related information is valuable to cybercriminals, who can use personal and demographic information, financial statements, health details and insurance information for identity theft, insurance fraud, financial gain or even blackmail, according to Don Duncan, security engineer for NuData Security.

"With healthcare information, cybercriminals can pose as doctors and patients to put in false claims or even change the records of patients," he said, via email. "This poses a severe danger to patients' health and to their pocketbooks. Additionally, there is no mechanism in place to address records that have been altered."

Source: https://threatpost.com/amca-healthcare-hack-widens-opko/145453/

4. Man Gets 51 Months in Prison for $10M BEC Fraud, Romance Scam

Muftau Adamu was sentenced on June 7, 2019 to 51 months in prison — 4 years and three months — for stealing more than $10 million through romance scams and business email compromise (BEC) fraud schemes aided by four other co-conspirators, between 2014 and 2018.

The fraud proceeds were collected by Adamu (aka Muftau Adams, aka Muftau Iddrissu) in collaboration with four other members of a criminal enterprise based in Ghana as detailed in the February 12 indictment released by the Department of Justice when he pleaded guilty to conspiracy to commit wire fraud.

"Muftau Adamu and his co-defendants conspired with others in Ghana to steal millions of dollars from businesses and vulnerable individuals across the United States through business email compromises and romance scams," said Manhattan U.S. Attorney Geoffrey S. Berman.

Besides the prison term, Adamu also got "three years of supervised release and ordered to forfeit $114,281.51 and pay restitution of $443,000 to victims."

Tourey Ahmed Rufai and Prince Nana Aggrey, two other members of the criminal group, were also sentenced to 48 months and 30 months in prison respectively, on April 12 and May 10. They also face three years of supervised release and have to forfeit funds and pay restitution to the victims.

"These five defendants admitted to participating in a conspiracy that involved stealing millions of dollars from U.S. businesses and individuals across the United States and laundering that money to their co-conspirators in Ghana through a network of bank accounts in the Bronx, many of which were opened using fake names and businesses," also said Berman on February 12.

Business email compromise fraud schemes

The criminal group targeted companies from all over the United States as part of their business email compromise fraud operations, attempting to trick employees from financial departments to wire funds to bank accounts they controlled.

"First, members of the Enterprise created email accounts with slight variations of email accounts used by employees of a victim company or third parties engaged in business with a company to 'spoof' or impersonate those employees or third parties," says the indictment.

The deceiving emails sent to their victims contained "fake authorization letters for the wire transfers that contained forged signatures of company employees."

This allowed the criminals to eventually convince some of their targets to wire hundreds of thousands of dollars into accounts under the control of Adamu, Rufai, and Aggrey.

BEC (also known as Email Account Compromise - EAC) scams are a widespread attacks used by crooks to quickly pilfer money from businesses.

BEC fraud schemes usually do not require a lot of technical skill seeing that they are focused on deceiving victims using social engineering into wiring their companies' funds to trusted entities whose bank accounts were swapped with ones controlled by the criminals prior to the attack.

The romance scams

To run the romance scam operations, the criminal enterprise sent electronic messages using "email, text messaging, or online dating websites," attempting to trick their targets which were

single men and women over 60 who lived alone that they involved into a romantic relationship with the scammers, via a fake identity proxy.

As detailed in the indictment, after the fraudsters "gained the trust of the victims using the fake identity, they used false pretenses to cause the victims to wire money to bank accounts the victims believed were controlled by their romantic interests, when, in fact, the bank accounts were controlled by members of the Enterprise."

The criminal group also convinced their romance scam victims to let the scammers use their bank accounts to store illegal proceeds from other illegal operations, funds which were later sent to other accounts controlled by the group.

"The members of the Enterprise, posing as the romantic interest of the victims, also introduced the victims to other individuals purporting to be, for example, consultants or lawyers, who then used false pretenses to cause the victims to wire money to bank accounts controlled by members of the Enterprise," also says the indictment.

On the whole, the scam group was able to pilfer over $10 million from their victims, money which ended up in the scammers' bank accounts from Bronx, New York, accounts opened using "fake names, stolen identities, or shell companies in order to avoid detection and hide the true identities of the members of the Enterprise controlling those accounts."

Source: https://www.bleepingcomputer.com/news/security/man-gets-51-months-in-prison-for-10m-bec-fraud-romance-scam/

5. Improving Safety in Schools Through the Convergence of Digital and Physical Security

This is a summary of a byline article written for eSchoolMedia.com by Fortinet's Vice President of Strategy and Analytics, Jonathan Nguyen-Duy. The entire article can be accessed here.

K-12 schools are under increasing pressure to protect the personal information of their students, along with the safety of the students themselves. Converging physical and cybersecurity is critical for student safety as well as enabling network performance and secure education.

> *"K-12 classrooms have embraced new learning initiatives through digital transformation efforts, including BYOD programs and e-learning strategies. In order to make the most out of these digitally-centered curriculums, IT teams must be able to provide students and staff with a seamless experience so as to not hinder learning opportunities. This includes things like high bandwidth, roaming through and between school environments, and supporting devices that transition between home and school."*

– Jonathan Nguyen-Duy, eSchoolMedia.com, May 06, 2019

K-12 schools are also popular targets for cybercriminals looking to steal data and exploit resources. So, in addition to performance issues, extra care must be taken to protect connected devices against viruses, data breaches, and malware.

But that is only part of the equation. Digital resources can also be used to provide for the physical safety of students. These include things like surveillance cameras, digitally controlled access points such as exterior and classroom doors, motion detectors, automated alarm systems, and facial recognition software that can alert administrators and security personnel of potential intruders and take measures to contain them.

> "*While these technology-based physical security tools offer important benefits in regards to education and safety, they also present new risks due to the expanded attack surface created by the connection of these new devices to campus networks*."

– Jonathan Nguyen-Duy, eSchoolMedia.com, May 06, 2019

However, cybercriminals are also increasingly targeting things like surveillance cameras in order to do things like "interfere with private conversations, gain access to cyber systems to steal information or launch an attack, and even shut cameras off, putting students' safety at risk." In fact, at the end of 2018, six of the top 12 global exploits identified and ranked by FortiGuard Labs threat research were targeting IoT devices – and four out of those top 12 were IP-enabled cameras. Likewise, "other cyber-connected systems, such as physical entryways and digitally controlled physical countermeasures to lock down facilities and isolate intruders, present similar vulnerabilities and risks."

Finally, compliance must be a top consideration as K-12 schools are required to demonstrate compliance with regulations such as CIPA, FERPA, and COPPA in order to protect students and their personal data.

Digital and Physical Security in K-12 Programs

Because K-12 security requirements are so complex and dynamic, traditionally isolated point products simply cannot keep up.

> "*This is compounded by the fact that many schools lack the security personnel required to keep up with the changing threat landscape, adding to the challenge of cybersecurity in these environments. The integration of physical security solutions, such as surveillance cameras and badge readers, with network security requires additional controls designed to recognize and respond to threats. By operating cameras on Next Generation Firewalls (NGFWs), for example, these devices would be protected against hacking attempts and other threats."*

– Jonathan Nguyen-Duy, eSchoolMedia.com, May 06, 2019

While consolidating physical security solutions into the network is a critical step towards providing comprehensive security for students and faculty, IT teams need to ensure that

network bandwidth can support complete availability, such as uninterrupted video streaming. They also need to ensure that firewall protection spans from the core to the outermost edges of the network to effectively defend against external attacks.

To achieve this level of protection, IT teams must understand which solutions can safely be utilized. Employing a high-performance surveillance solution that is fully-integrated you're your cybersecurity resources—such as the FortiCamera—protection is guaranteed because all elements are purpose-built and hardened to withstand cyberthreats.

Final Thoughts

Without proper security measures in place, K-12 schools are likely to face cyberattacks which not only put the personal information of students and staff at risk, but that can also compromise physical security solutions that can put the physical safety of individuals at risk.

Despite the benefits that physical security solutions can offer, therefore, it is critical that these solutions be securely integrated into the network so they can effectively defend against both cyber and physical threats—all while ensuring that performance is never compromised.

Source: *https://www.fortinet.com/blog/industry-trends/digital-physical-security-convergence-in-education.html*

6. Multiple Linux and FreeBSD DoS Vulnerabilities Found by Netflix

A denial of service flaw found in the way recent Linux kernels handle TCP networking can be exploited by remote attackers to trigger a kernel panic in vulnerable systems.

In all, Netflix Information Security's Jonathan Looney found three Linux vulnerabilities, two related to "the minimum segment size (MSS) and TCP Selective Acknowledgement (SACK) capabilities," and one related only to MSS, with the most serious one named SACK Panic being the one that can cause affected systems to panic and reboot.

As per Red Hat, the issues which impact the kernel's TCP processing subsystem are tracked via multiple CVEs, with CVE-2019-11477 SACK Panic having been assigned an important severity with a 7.5 CVSS3 base score, while CVE-2019-11478 and CVE-2019-11479 are considered to be moderate severity vulnerabilities.

Patches are already available as detailed in Netflix's NFLX-2019-001 security advisory, with mitigation measures also being available for machines where patching is not an immediate or easy option.

The SACK Panic security flaw

The SACK Panic vulnerability (Debian, Red Hat, Ubuntu, Suse, AWS) impacts Linux kernels 2.6.29 and later, and it can be exploited by "sending a crafted sequence of SACK segments on a TCP connection with small value of TCP MSS" which will trigger an integer overflow.

To fix the issue, "Apply the patch PATCH_net_1_4.patch. Additionally, versions of the Linux kernel up to, and including, 4.14 require a second patch PATCH_net_1a.patch," says Netflix Information Security's advisory.

To mitigate the issue, users and administrator can completely disable SACK processing on the system (by setting /proc/sys/net/ipv4/tcp_sack to 0) or block connections with a low MSS using the filters provided by Netflix Information Security HERE — the second mitigation measure will only be effective when TCP probing is also disabled.

More denial of service vulnerabilies

The other two vulnerabilities impact all Linux versions, with CVE-2019-11478 (dubbed SACK Slowness) being exploitable by sending "a crafted sequence of SACKs which will fragment the TCP retransmission queue," while CVE-2019-11479 allows attackers to trigger a DoS state by sending "crafted packets with low MSS values to trigger excessive resource consumption."

CVE-2019-5599 is the FreeBSD counterpart of CVE-2019-11478, it impacts FreeBSD 12 installations using the RACK TCP Stack and it can be abused by delivering "a crafted sequence of SACKs which will fragment the RACK send map."

Luckily, as explained by FreeBSDHelp, FreeBSD 12 does not have RACK enabled by default and requires a custom kernel to be toggled on.

Linux and FreeBSD admins and users can fix the first one can by applying PATCH_net_2_4.patch, and the second one with the PATCH_net_3_4.patch and PATCH_net_4_4.patch security patches. CVE-2019-5599 can be patched by applying "split_limit.patch and set the net.inet.tcp.rack.split_limit sysctl to a reasonable value to limit the size of the SACK table."

As workarounds, both CVE-2019-11478 and CVE-2019-11479 can be mitigated by blocking remote network connections with a low MSS with Netflix Information Security-supplied filters available HERE — applying the filters might subsequently break low MMS legitimate connections. The FreeBSD flaw can be mitigated by simply toggling off the RACK TCP stack.

"*The extent of impact is understood to be limited to denial of service at this time. No privilege escalation or information leak is currently suspected,*" says Red Hat.

"*Good system and application coding and configuration practices (limiting write buffers to the necessary level, monitoring connection memory consumption via SO_MEMINFO, and aggressively closing misbehaving connections) can help to limit the impact of attacks against these kinds of vulnerabilities,*" also notes Netflix Information Security in its advisory.

Source: *https://www.bleepingcomputer.com/news/security/multiple-linux-and-freebsd-dos-vulnerabilities-found-by-netflix/*

7. The U.S. Loses Over $1.5 Trillion in a Decade of Data Breaches

A decade's collection of data breaches shows a bleak picture with billions of records exposed in this type of incidents and financial damages of more than $1.6 trillion.

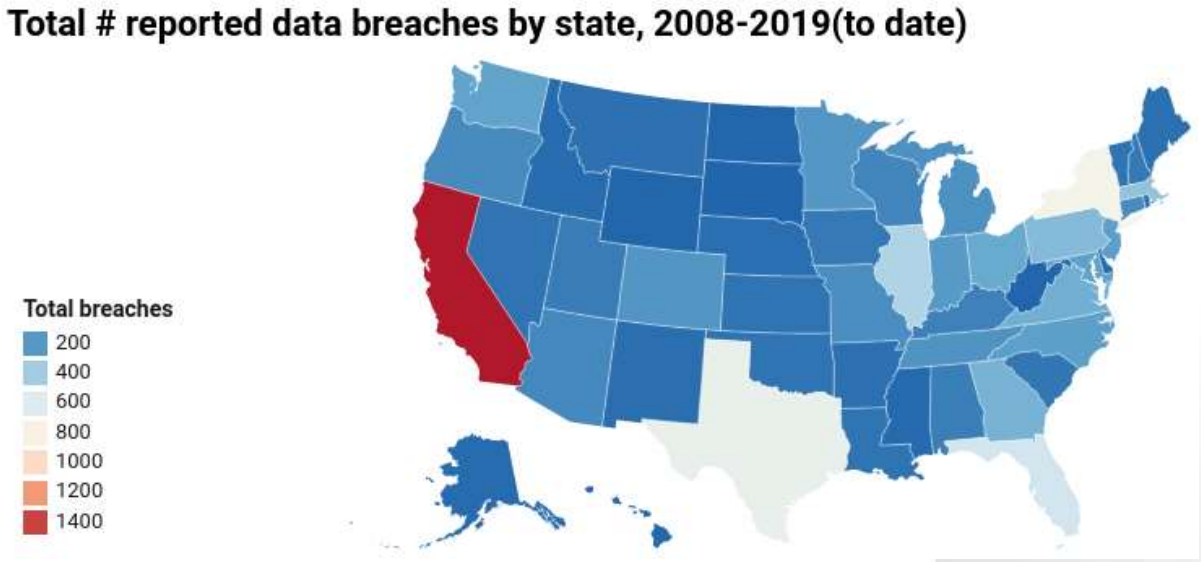
Data collected from public sources reveal that since 2008 there were close to 9,700 breach events in the U.S., involving more than 10.7 billion records, with an average cost calculated in 2018 at $148 per record.

Open-source info outlines sad situation

The information relies only on details made public by state-based sources and in media reports. The figures are likely conservative as data breach disclosure laws differ from one state to another; in some cases, even notifying the individuals whose data was exposed is not a requirement.

"Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years." - New Jersey security breach disclosure act.

The details were compiled by researchers at Comparitech, who broke it down per state to determine the regions that were affected the most by data breach incidents. The data includes both a tally of the events and of the records exposed.



According to the report, California is the state with the most publicly documented breaches, and also one where consumer privacy is taken seriously. 1,493 incidents affected 5.59 billion personal records.

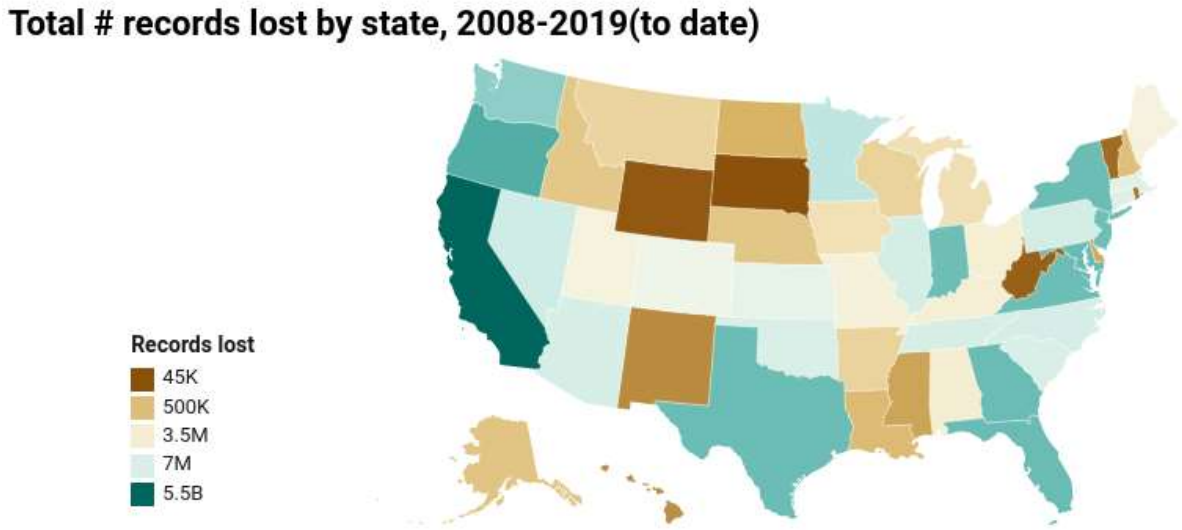
It is worth noting that the state law requires that a sample copy of a breach notice to be submitted to the Attorney General if more than 500 California residents are affected.

Taking second place is the state of New York. Comparitech found 729 data breach incidents that were publicly documented over the past decade. The records exposed this way amounted to 293 million.

Close behind is Texas, with 661 events and 288 million records exposed. Most of the personal information came from unauthorized access in 2011 of up to 250 million email addresses and names managed by marketing company Epsilon. The firm acknowledged the intrusion.

As one may observe, there isn't always a balance between the records exposed and the number of breaches. Data Comparitech collected for Oregon shows that the state suffered at least 157 data security incidents that exposed 1.37 billion records.

Most of the email info came from a faulty backup event in 2017 impacting a fake marketing company called River City Media (RVC). Researchers at MacKeeper said at the time that RVC was a spam factory "responsible for up to a billion daily email sends."



As we mentioned before, the figures presented in Comparitech's report are only a minimum. The researchers agree that the real numbers are higher as some breach reports do not disclose the number of records exposed; furthermore, the information "might be unknown or below the threshold imposed by the state," or new details may emerge at a later date.

For instance, it was revealed this week that a phishing attack in January at the Department of Human Services (DHS) in Oregon impacted data belonging to 645,000 individuals. Although the attack was reported in March, the complete number of people impacted could only be roughly estimated at that time.

Comparitech makes available in an online document a complete list with publicly reported data breaches they found for each state.

Source: https://www.bleepingcomputer.com/news/security/the-us-loses-over-15-trillion-in-a-decade-of-data-breaches/

8. Desjardins Group Data Leak Exposes Info of 2.9 Million Members

Sensitive personal information of roughly 2.9 million Desjardins Group members was leaked after an employee disclosed it to people outside the organization without authorization.

Desjardins Group is the largest association of credit unions in North America and, according to its official Twitter account, also the largest cooperative financial group in Canada.

As detailed by the company in a press release, "The disclosed information of Personal members is comprised of: first and last name, date of birth, social insurance number, address, phone number, email address and details of banking habits and Desjardins products."

In the case of business members, the leaked data included "business name, business address, business phone number, owner's name and names of users on the AccèsD Affaires account," with "some of the personal information associated with AccèsD Affaires account users" probably also exposed.

Desjardins became aware of the data leak on June 14, 2019, when "the Laval police provided Desjardins with information confirming that the personal information of more than 2.9 million members (including 2.7 million personal members and 173,000 business members) had been disclosed to individuals outside the organization."

Breach not caused by a cyberattack

After discovering the data leak, Desjardins notified the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec and the Autorité des marchés financiers, and fired the ill-intentioned employee behind the incident.

Despite the huge data leak it experienced, the company reassured its clients saying that:

- Desjardins has not been the target of a cyberattack. Our computer systems have not been compromised in any way by this incident.
- We understand that this is a worrying situation. We sincerely regret the inconvenience it has caused. Your assets and accounts at Desjardins are protected—you won't suffer a financial loss if unauthorized transactions are made in your Desjardins accounts as a result of this situation.

The Canadian cooperative financial group says that its members' "passwords, security questions, PINs, and credit and debit card numbers have not been compromised" in the data leak.

"This is a first for Desjardins, and we will do everything in our power to make sure it's the last. Unfortunately, no company is fully protected from attempts to steal personal information," the company also noted in the press release.

Desjardins stated that it will pay for a 12-month credit monitoring plan for all members who have been affected in the incident:

Members who have been affected can also find more information on how to minimize identity theft risks HERE.

Source: https://www.bleepingcomputer.com/news/security/desjardins-group-data-leak-exposes-info-of-29-million-members/

9. Millions of Dell PCs Vulnerable to Flaw in Third-Party Component

Millions of PCs made by Dell and other OEMs are vulnerable to a flaw stemming from a component in pre-installed SupportAssist software. The flaw could enable a remote attacker to completely takeover affected devices.

The high-severity vulnerability (CVE-2019-12280) stems from a component in SupportAssist, a proactive monitoring software pre-installed on PCs with automatic failure detection and notifications for Dell devices. That component is made by a company called PC-Doctor, which develops hardware-diagnostic software for various PC and laptop original equipment manufacturers (OEMs).

"According to Dell's website, SupportAssist is preinstalled on most of Dell devices running Windows, which means that as long as the software is not patched, this vulnerability probably affects many Dell users," Peleg Hadar, security researcher with SafeBreach Labs – who discovered the breach – said in a Friday analysis.

A patch has been issued by PC-Doctor that fixes impacted devices. Impacted customers can find the latest version of SupportAssist here (for single PC users) or here (for IT managers).

Dell sought to downplay the flaw, telling Threatpost that customers are urged to turn on automatic updates or manually update their SupportAssist software. Because most customers have automatic updates enabled, around 90 percent of customers to date have received the patch, said a Dell spokesperson.

"Our first priority is product security and helping our customers ensure the security of their data and systems," the spokesperson said. "The vulnerability discovered by SafeBreach is a PC Doctor vulnerability, a third-party component that ships with Dell SupportAssist for Business PCs and Dell SupportAssist for Home PCs. PC Doctor moved quickly to release the fix to Dell, we implemented it and released updates on May 28, 2019 for the affected SupportAssist versions."

The vulnerability stems from a component in SupportAssist, which checks the health of system hardware and software and requires high permissions. The vulnerable PC-Doctor component is a signed driver installed in SupportAssist. This allows SupportAssist to access the hardware (such as physical memory or PCI).

The component has a dynamic link library (DLL) loading vulnerability glitch that could allow a malicious actor to load an arbitrary unsigned DLL into the service. A DLL is a file format used for holding multiple processes for Windows programs.

When loading a DLL into the program, "No digital certificate validation is made against the binary," said Hadar. "The program doesn't validate whether the DLL that it will load is signed. Therefore, it will load an arbitrary unsigned DLL without any hesitation."

Because the PC-Doctor component has signed certificates from Microsoft for kernel-mode and SYSTEM access, if a bad actor is able to load the DLL they would achieve privilege escalation and persistence – including read/write access to low-level components including physical memory, System Management BIOS, and more.

Hadar told Threatpost that a remote attacker could exploit the flaw. All that the bad actor would need to do is persuade the victim to download a malicious file (using social engineering or other tactics) to a certain folder.

"The required privileges are depends on the 'PATH env' variable of the user, if he has a folder which a regular user can write to, no high privileges are necessary," Hadar told Threatpost."After an attacker exploits the flaw he gains execution as SYSTEM within a signed service, basically he can do whatever he wants, including using PC-Doctor signed kernel driver in order read and write physical memory."

Making matters worse, the component in SupportAssist also impact an array of other OEMs who are using rebranded versions of it – meaning that other unnamed OEM devices are vulnerable as well, said security researchers with SafeBreach Labs.

PC-Doctor did not disclose who the other impacted OEMs are, but did say that patches have been released to address "all affected products."

"PC-Doctor became aware of an uncontrolled search path element vulnerability in PC-Doctor's Dell Hardware Support Service and PC-Doctor Toolbox for Windows," a PC-Doctor spokesperson told Threatpost. This vulnerability allows local users to gain privileges and conduct DLL hijacking attacks via a trojan horse DLL located in an unsecured directory which has been added to the PATH environment variable by a user or process running with administrative privileges. PC-Doctor takes software security seriously and as such has already released updates to all affected products to address the issue."

Source: *https://threatpost.com/millions-of-dell-pcs-vulnerable-to-flaw-in-third-party-component/145833/*

10. Phishing Websites Increase Adoption of HTTPS

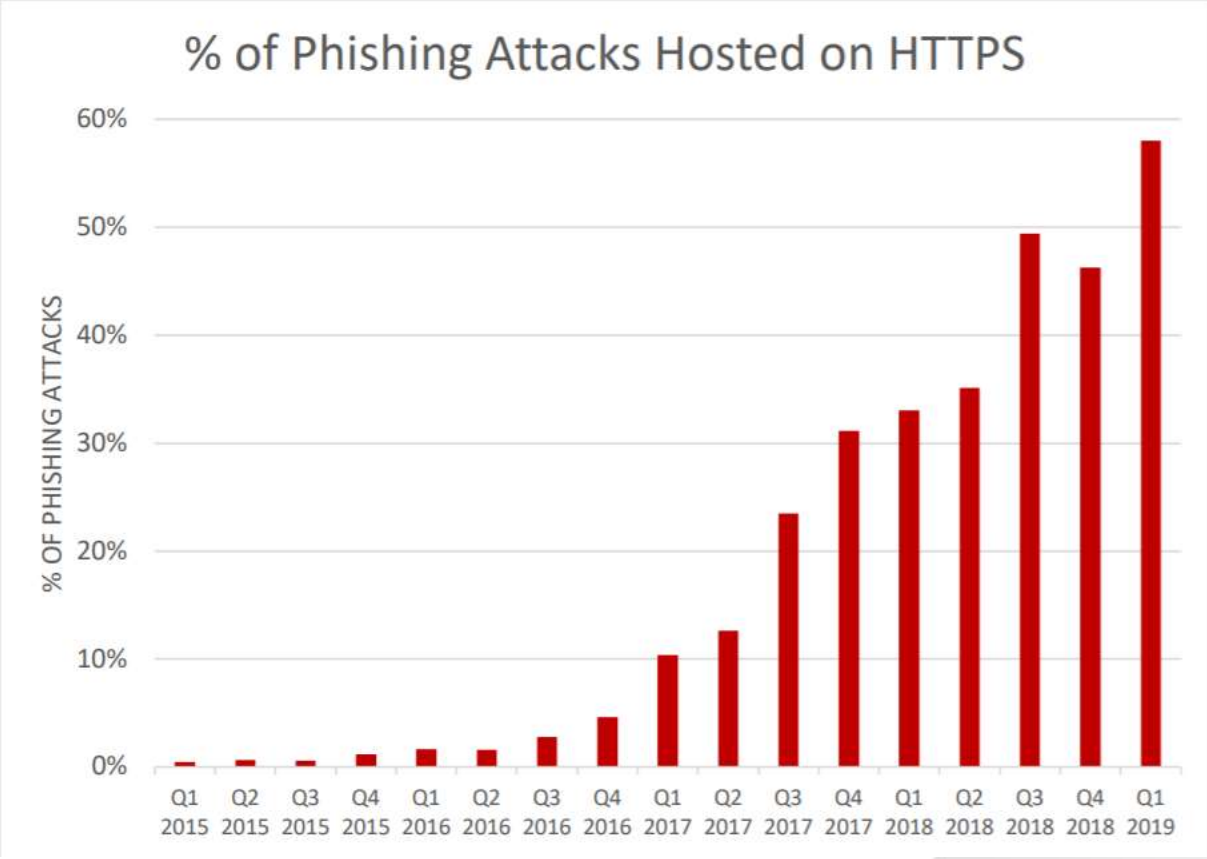
As the adoption of cryptographic protocols for secure website communication increased, cybercrooks also moved to HTTPS to keep their operation floating.

Over half of the phishing websites detected in the first quarter of the year used digital certificates to encrypt the connections from the visitor. This is a trend that kept growing since mid-2016.

HTTPS is designed to protect user privacy by encrypting the traffic between a website and the browser. This prevents third parties from viewing the data that's exchanged. It started as a defense against snooping traffic on pages with forms for sensitive information (payment card details, logins) and soon became a communication standard for the entire website.

Crooks catch up on HTTPS adoption

Statistics from PhishLabs - a company that monitors phishing activity at a large scale, show that up to 58% of the phishing websites in the first months of 2019 were using the secure HTTP protocol. This is a 12% jump compared to the last quarter of 2018.



As browsers became more aggressive about HTTPS adoption by warning users when their connection is not secure, phishing scams had to follow the trend. Impersonating an HTTPS website is virtually impossible now without a TLS certificate.

If a while ago getting a digital certificate was both a complicated and expensive endeavor, the process became much easier lately and TLS certificates are now available even for free (https://letsencrypt.org/).

"Attackers can easily create free DV (Domain Validated) certificates, and more web sites are using SSL in general. More web sites are using SSL because of browsers warning users when SSL is not used, and most phishing is hosted on hacked, legitimate sites," says John LaCour, founder and CTO of PhishLabs.

The researchers expect the adoption of HTTPS to grow among cybercrooks as failing to do so would mean an end to their business.

Source: https://www.bleepingcomputer.com/news/security/phishing-websites-increase-adoption-of-https/

11. Malspam Campaigns Hide Infostealers in ISO Image Files

Multiple malicious campaigns observed in April concealed LokiBot and Nanocore malware inside ISO image files small enough to fit into an email attachment.

Both LokiBot and Nanocore incorporate data-stealing capabilities. They target web browsers, email clients, remote admin tools (SSH, VNC, and RDP), and clipboard data. They can also collect information about documents present on the system and monitor user keystrokes to extract more sensitive details.

Security researchers discovered 10 variants of this type of campaign, with variations in the ISO images and messages delivered to potential victims. The endeavors appear to follow the "spray and pray" principle as they did not target specific individuals or businesses.

ISO files are less suspicious

The ISO approach makes sense from an attacker's perspective as most modern operating systems can automatically mount the images and show their content when the user accesses them.

Moreover, some security solutions tend to whitelist ISO files for performance reasons, thus making them less susceptible to detection.

Researchers at Netskope noticed that the ISO files ranged in size from 1MB to 2MB, a small weight for this type of archive, which typically is larger than 100MB.

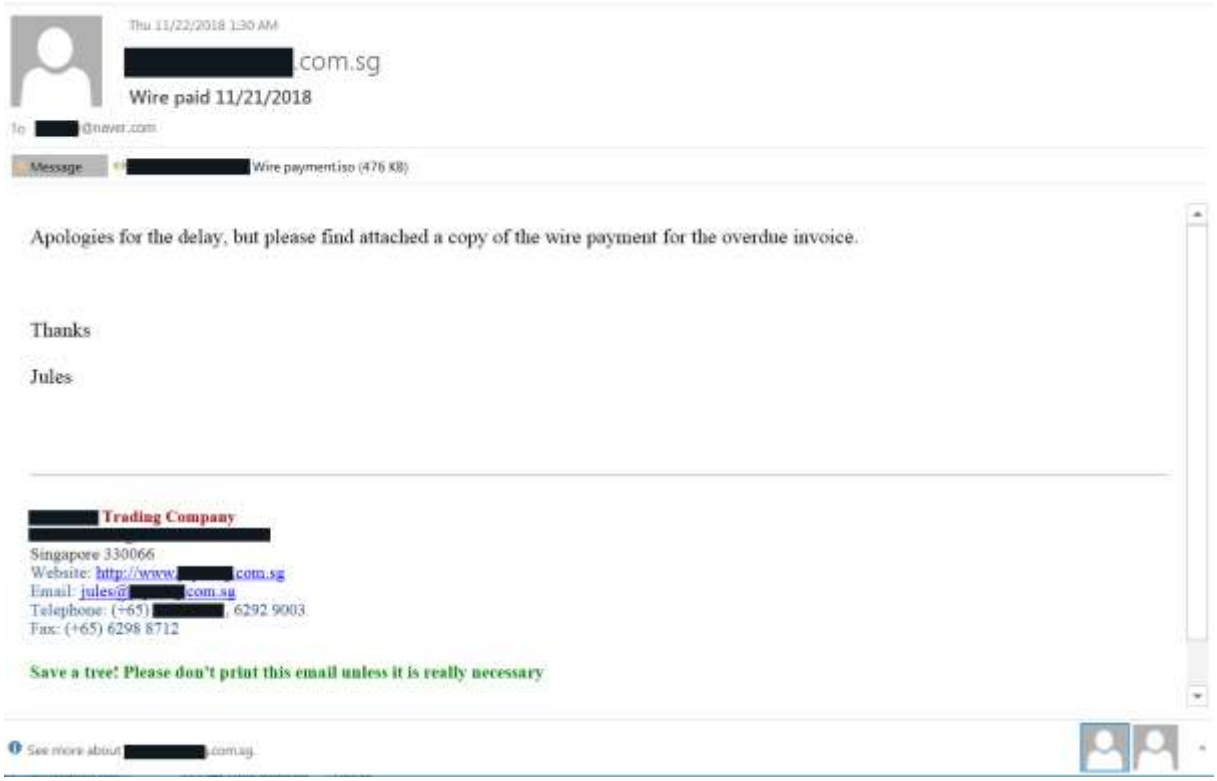
"The image contains only one executable file embedded in it which is the actual malware payload," they write in a report published today.

The payment document trick

The generic spam email delivering LokiBot or Nanocore RATs uses the wire payment ruse to lure the user into opening the allegedly financial document in the attachment.

"Apologies for the delay, but please find attached a copy of the wire payment for the overdue invoice," reads the message.

As seen in the sample below, the attacker put in the effort to add a signature that appears to be from a real company, complete with its address, website, and contact details of the sender.



The version of LokiBot delivered this way is similar to previously seen variants of the malware. However, the threat comes with some anti-reversing techniques to prevent its analysis.

Netskope analyzed a strain that used the "IsDebuggerPresent()" function to determine if it is loaded inside a debugger.

Its developers also implemented techniques designed to recognize if the malware runs in a virtual machine: "measuring the computational time difference between CloseHandle() and GetProcessHeap()."

The Nanocore variant used in the campaigns discovered by Netskope is not new and has been used for malicious activities as far back as 2017.

Both threats are regularly seen in business email compromise (BEC) scams from Nigerian attackers that researchers at Palo Alto Networks dubbed SilverTerrier.

Their popularity slowly increased over the past two years, with LokiBot being the top info-stealing malware used by SilverTerrier last year, and Nanocore being in the top ten list of preferred remote administration tools (RATs).

Source: https://www.bleepingcomputer.com/news/security/malspam-campaigns-hide-infostealers-in-iso-image-files/

12. Attackers Earn Over $1 Million in Florida Ransomware Attacks

Hackers launching ransomware attacks against municipalities in Florida locked earnings in excess of $1 million this month as administrators of two cities found no other way to recover files on affected systems.

Following a ransomware attack - dubbed "Triple Threat" because it mixes three methods of compromise - on June 10, the computers of the City of Lake City ceased to function as the malware encrypted the data on them.

Quick reaction does not prevent infection

The attackers demanded a ransom of 42 Bitcoins, which is over $530,000 at today's value, to provide the decryption keys that would restore the data.

Disconnecting the affected systems minutes after the infection did not prevent the malware from impacting most land-line phones and email systems, forcing employees to use pen and paper to continue their activity.

Emergency services, like those used by the police and the fire department, remained unaffected because they were on a separate network.

"Our systems are shut down, but there is no evidence to indicate any sensitive data has been compromised. All customer service payment data, such as credit card data, is stored off-site by third-party vendors and would not have been accessed by an attack like this on our network," said City Information Technology Director Brian Hawkins.

With no proper backup to restore the data from, Lake City was left with no option but to pay the ransom; the bitcoins were sent to the hackers on Tuesday. Mayor Stephen Witt said that the administration took this decision after talking with the FBI and the city's insurance company.

Witt says that most of the money is covered by the insurance save for $10,000, which will be supported by the citizens by paying a higher insurance rate in the future.

Another Florida city agreed to pay the ransom

Last week, Riviera Beach city also in Florida gave into a ransomware demand after data on its computers was locked in an incident on May 29.

Paying the hackers was voted unanimously in a City Council meeting as lack of proper backup procedures left the administration with no other choice.

In this case, the attackers asked for 65 bitcoins, which was around $600,000 at the time of the decision.

The decision came after the city already approved spending close to $1 million on new computers and hardware that would help rebuild the IT network.

Both incidents occurred because an employee ushered in the malware by opening a malicious email and backup policies and systems, if they were available, did not work properly.

In total, the hackers behind these two attacks collected 107 bitcoins that are currently worth about $1,36 million.

Security experts and law enforcement do not encourage parties affected by ransomware to pay the hackers. This only encourages them to launch more attacks and there is no guarantee that they will actually deliver the decryption key.

Source: https://www.bleepingcomputer.com/news/security/attackers-earn-over-1-million-in-florida-ransomware-attacks/

13. Cisco Patches Critical Flaws in Data Center Network Manager

Cisco released today patches for its Data Center Network Manager (DCNM) software fixing critical vulnerabilities that allow a remote attacker to upload files and execute actions with root privileges.

The updates cover four security bugs, two of them standing out through a close-to-maximum severity score of 9.8 out of 10.

All vulnerabilities are in DCNM's web-management console and can be exploited remotely by a potential adversary without the need to authenticate.

DCNM is Cisco's solution for maintaining visibility and automating the management of networking gear in data centers, such as Nexus Series switches.

Critical flaws lead to increased privileges

One of the critical issues is tracked as CVE-2019-1620. It exists in DCNM versions prior to version 11.2(1) and could be exploited by a threat actor to upload arbitrary files on an affected system.

Incorrect permission settings in the web-based interface of the network management platform make it possible to write files on the filesystem and run code with root privileges.

"An attacker may achieve creation of arbitrary files on the underlying DCNM filesystem by sending specially crafted data to a specific web servlet that is available on affected devices," reads Cisco's advisory.

The company notes that an attacker cannot leverage the bug without authentication in DCNM 11.0(1) and earlier. In versions starting 11.1(1) the affected web servlet supports unauthenticated access.

The second critical vulnerability is identified as CVE-2019-1619 and a potential adversary could use it on releases before 11.1(1) to bypass authentication and get admin privileges. A session cookie can be obtained by sending a specially crafted HTTP request to a specific web servlet.

Less severe, not less important

Another bug - high severity score of 7.5 - that could be exploited to do sufficient damage is CVE-2019-1621. It stems from incorrect permission settings in the web-based interface of DCNM 11.2(1) and earlier.

"An attacker could use a specific web servlet that is available on affected DCNM devices to download arbitrary files from the underlying filesystem" by requesting specific URLs, Cisco informs today.

The least severe vulnerability Cisco patched today in DCNM is CVE-2019-1622, a medium risk information disclosure that allows potential adversaries to download log data and diagnostic info from an affected device.

Cisco credits independent researcher Pedro Ribeiro for discovering the glitches and reporting them through Accenture's iDefense Vulnerability Contributor Program.

Source: https://www.bleepingcomputer.com/news/security/cisco-patches-critical-flaws-in-data-center-network-manager/

14. Criminals, ATMs and a cup of coffee

In spring 2019, we discovered a new ATM malware sample written in Java that was uploaded to a multiscanner service from Mexico and later from Colombia. After a brief analysis, it became clear that the malware, which we call ATMJaDi, can cash out ATMs. However, it doesn't use the standard XFS, JXFS or CSC libraries. Instead, it uses the victim bank's ATM software Java proprietary classes: meaning the malware will only work on a small subset of ATMs. It makes this malware very targeted.

Kaspersky products detect the sample as Trojan.Java.Agent.rs

Technical Details

First, as with most other ATM malware, the attackers must find a way to install the malware on the target ATMs. The malware can't be controlled via the ATM keyboard or touchscreen, because it runs a self-crafted HTTP server web interface for its purpose. So the criminals must have network access to the target ATM. This makes us believe that the criminals have

compromised the bank's infrastructure to gain access to the network that the ATMs are connected to.

Once installed and executed, the malware, in the form of a Java archive file called "INJX_PURE.jar", looks for the process that controls the ATM and injects itself into it, giving it control of the legitimate ATM process. After injection, the malware prints a message on the terminal simultaneously in several languages: Russian, Portuguese, Spanish and Chinese. However, all the other messages or strings used by the malware are in English. The different language phrases shown in the output can be translated into English as "Freedom and glory". This is followed by the additional Russian message "отдельный", which means "separate". We believe this might be a false flag, because native Russian speakers would never use this word in this context.

- Свобода и слава
- Liberdade e glória
- Libertad y gloria
- 自由与荣耀
- отдельный

Next, an HTTP server is started that accepts commands using predefined URL paths. They are:

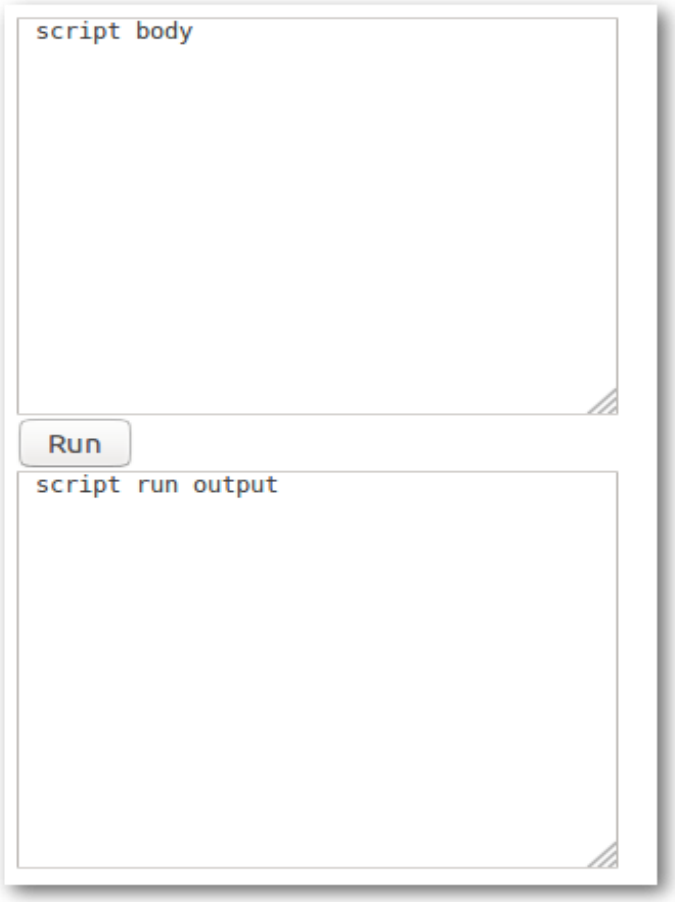
- **/d** to dispense or to get the ATM cassette to carry out actions (the proper action is determined by the passed parameters);
- **/eva** to evaluate (run) user-supplied code on the victim ATM;
- **/mgr** for the manager, which gives criminals access to a list of all running classes for the attached Java virtual machine, so that they can call any function they desire, supplying the arguments if needed;
- **/core** allows the criminals to load a specified *.jar* file from the victim file system;
- **/root** path accepts a POST request body and passes it as a shell command to cmd.exe, returning the resulting output.

The dispensing and "run a shell" path do not have an interface page with forms and buttons, but instead only accept pre-prepared HTTP POST requests and print the raw text results to a page, omitting HTML tags. So, in the case of the dispensing request, the malware response will be the 'ok' string. The "get cash units information" request will be followed by a string describing the ATMs cash units status (see the example below).

1:1000;5:700;10:100;20:30;

This string consists of four groups, each group separated with a semicolon. It is a list that corresponds to the ATM cash cassette and consists of two values, separated by a colon: the denomination and the actual number of bills in the cassette. In the example above, the first cassette has 1000 banknotes of denomination 1, 700 banknotes of denomination 5, etc.

Other than the “run a shell”, “dispense” and “get cash unit”, the “eva”, “mgr” and “core” paths have interface pages. Below is a screenshot of the evaluation page:



/eva path interface example screenshot

It allows the criminals to paste and run any JavaScript code on a victim ATM and see what it returns. Why JavaScript? Because Java allows the use of external engines, and the criminals used a JavaScript one. Below is the function that the malware uses to run the passed JavaScript code.

```
public static String runjs(String script)
{
  ScriptEngineManager manager = new ScriptEngineManager(HTTPServ.class.getClassLoader());
  ScriptEngine engine = manager.getEngineByExtension("js");
  StringWriter sw = new StringWriter();
  PrintWriter pw = new PrintWriter(sw);
  engine.getContext().setWriter(pw);
  engine.getContext().setErrorWriter(pw);
  try
  {
     engine.eval(script);
  }
  catch (ScriptException e)
  {
     e.printStackTrace(pw);
  }
  String outx = sw.getBuffer().toString();

  return outx;
}
```

Malware sample code that can evaluate JavaScript

Conclusions

The targeted nature of ATMJaDi shows that the criminals studied the victim very well before writing their malware. It's clear that they must have had access to an ATM where the custom Java classes were running and most likely to the Java program source code as well.

Also, the way the malware can be controlled shows that the criminals planned to gain network access to the infected ATM, most likely through the bank's internal network.

What banks can do to prevent these types of attacks:

- Set up special anti-targeted attack solutions such as KATA (Kaspersky Anti Targeted Attack Platform) to protect the bank's network and other solutions to protect ATMs from malware;
- ATM file whitelisting;
- The bank ATM network has to be isolated and access to it must be highly restricted;

This is not a complete list of actions: the issue of information security requires constant attention and action.

Source: https://securelist.com/criminals-atms-and-a-cup-of-coffee/91406/

If you want to learn more about ASOC and how it can improve your security posture, contact us at: **asoc.sales@telelink.com**

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.