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

Monthly Security Bulletin

February 2019

Table of Contents:

Executive Summary

- "A database of breached emails totaling 773 million unique addresses has turned up on a popular underground hacking forum, giving cybercriminals one of the largest jackpots ever seen when it comes to account-compromise efforts." The jackpot presupposes security treats to both private citizens and companies. To learn more ***Jump to article*.**
- "The European Commission in January is funding 14 bug bounty programs in hopes of sniffing out vulnerabilities in the free open source projects that EU institutions rely on. The bug bounty programs span 14 open source software projects and offers a total of almost $1 million for all bounties combined." To learn more ***Jump to article*.**
- "Threat actors in the phishing business have adopted a new technique to obfuscate the source code for the forged page by using a custom web font to implement a substitution cipher that looks like plaintext." To learn more ***Jump to article*.**
- Malicious actors have had access to the Marriott's Starwood reservation database since 2014 and that they've had had access to data such as passport numbers, Starwood Preferred Guess account details, date of birth, gender, arrival and departure information, reservation date, and communication preferences. Although significantly lower than the initially expected 383 million affected customers, the 5.25 million is a number large enough to be frightening. To learn more ***Jump to article*.**
- With the rising need to protect privacy and sensitive data, more and more traffic is being encrypted. "This is a good thing from both a security and privacy perspective, but what if the encryption is being used to hide malicious activity on enterprise networks?" Are the decryption applications and devises being produced matching the latest security protocol versions? To learn more ***Jump to article*.**
- Aside of from affecting hundreds of thousands federal employees who were working without pay, the U.S. federal shutdown is also having negative affect on the cyber security of many .gov sites. Many have been rendered insecure or inaccessible due to expired transport layer security (TLS) certificates. The list includes "sensitive government payment portals and remote access services for organizations like NASA, the U.S. Department of Justice and the Court of Appeals." To learn more ***Jump to article*.**
- "The average cost estimate for cleaning up a cyberattack comes in at around $1.1 million, according to a recent survey. But this is actually a rosy view: For those organizations that actually calculate (versus estimate) the real cost of an attack, that number increases significantly to $1.67 million." To learn more ***Jump to article*.**
- Financial organizations in West Africa have been victims of cyber attacks since mid-2017. The malicious actors "rely on off-the-shelf malware, free hacking tools, and utilities already available on the target systems to steal credentials, install backdoors, and run commands". Some of the tools used, go for as little as 25$, although the use of more expensive ones, such as Cobalt Strike's pen testing tools has been observed. To learn more ***Jump to article*.**

- "France's National Data Protection Commission (CNIL) has fined Google $57 million (€50 million) for violations of the General Data Protection Regulation (GDPR) – the largest fine yet issued under the EU's new data privacy law." To learn more ***Jump to article***.
- "The Department of Homeland Security is ordering all federal agencies to urgently audit Domain Name System (DNS) security for their domains in the next 10 business days. The department's rare "emergency directive," issued Tuesday, warned that multiple government domains have been targeted by DNS hijacking attacks, allowing attackers to redirect and intercept web and mail traffic." To learn more ***Jump to article***.
- "An array of phishing emails harboring Word attachments with embedded macros have been infecting systems with a deadly malware and ransomware duo. The campaign, spotted by researchers at Carbon Black, has hit infected systems with a lethal attack combination that harvests credentials, gathers system and process information, and then encrypts data in order to extort payments from victims. To learn more ***Jump to article***.
- "A European Commission Statement says that Data Protection Authorities (DPAs) across Europe received 95,180 complaints regarding the mishandling of personal data and companies reported a record number of 41,502 data breaches since the General Data Protection Regulation (GDPR) was enacted on 25 May 2018." To learn more ***Jump to article***.
- January 28th, also known as the Data Privacy Day in the U.S. and Canada or Data Protection Day in Europe, since 1981. What it meant back then and how it has developed throughout the years? To learn more ***Jump to article***.
- "Organizations worldwide are struggling to keep up with cybercrime. Even though Gartner predicts worldwide spending on Information Security will reach $124 billion this year, security researchers estimate that the cost of cybercrime will outpace that spend by over 16X, reaching $2.1 trillion by the end of 2019." To learn more ***Jump to article***.
- Social Engineering Attacks and how trainings for them can improve the overall security posture of a company. The insides of an X-Force Red, IBM Security's team veteran hacker showing how to hack a company with a box of doughnuts. To learn more ***Jump to article***.

1. Cyber-Jackpot: 773M Credentials Dumped on the Dark Web

A database of breached emails totaling 773 million unique addresses has turned up on a popular underground hacking forum, giving cybercriminals one of the largest jackpots ever seen when it comes to account-compromise efforts.

Troy Hunt was first alerted to the cache, which totals 87GB of data, after it was seen being hosted on the MEGA cloud service (it has since been removed). The data was organized into 12,000 separate files under a root folder called "Collection #1," which gives the trove its name. Soon after that, the whole shebang turned up on the cyber-underground.

In examining the data, Hunt found that there are 1.16 billion unique combinations of email addresses and passwords listed. And after deduping and cleaning up the database, Hunt was left with about 773 million unique email addresses – the single largest collection of breached emails ever to be loaded into his compromised-credentials look-up service, Have I Been Pwned (HIBP).

There are also 21 million unique passwords in the database: "As with the email addresses, this was after implementing a bunch of rules to do as much clean-up as I could including stripping out passwords that were still in hashed form, ignoring strings that contained control characters and those that were obviously fragments of SQL statements," Hunt said in a posting on Thursday.

Thousands of Breaches

As for the sources of the data, there are literally thousands of compromises at the root of the database.

"The post on the forum referenced 'a collection of 2000+ dehashed databases and combos stored by topic' and provided a directory listing of 2,890 of the files," Hunt said.

This list includes a few previous breaches that Hunt recognized, but also others that are new. In all, out of about 2.2 million people that use HIPB's notification service, 768,000 of them are implicated in this data dump. And there are also around 140 million email addresses that HIBP has never seen before.

"This gives you a sense of the origins of the data but again, I need to stress 'allegedly,'" Hunt said. "I've written before about what's involved in verifying data breaches and it's often a non-trivial exercise…it's entirely possible that some of them refer to services that haven't actually been involved in a data breach at all."

In a comment to Threatpost, he elaborated: "The data contains breaches such as 000webhost and the Plex forum, or at least those names are on the list of alleged sources."

With so many different sources feeding into it, Collection #1 did not just appear one day, fully formed.

"Some of the breaches indicated go back many years (pre 2010), whilst I've had other people claim it had data from November last year," Hunt told Threatpost. "I've not verified that last claim, but certainly it's incidents spanning many years."

This could be very good news if those impacted regularly change their passwords.

"This massive collection of data harvested through data breaches has been built up over a long period of time, so some of the account details are likely to be outdated now," Sergey Lozhkin, security expert at Kaspersky Lab, told Threatpost. "However, it is no secret that despite growing awareness of the danger, people stick to the same passwords and even re-use them on multiple websites."

Data-Spill Timeline

What's clear is that the data was in broad circulation for some time before Hunt was aware of it, based on the number of people that contacted him privately and the fact that it was published to a well-known public forum.

"In terms of the risk this presents, more people with the data obviously increases the likelihood that it'll be used for malicious purposes," he said. After all, the longer criminals are able to use the data without consumers knowing about it, the more likely they are to succeed.

Those malicious purposes are likely to consist of credential-stuffing, which is a technique used by hackers to gain fraudulent access to an account. It uses automated scripts to try multiple username/password combos against a targeted website. Successful account compromises from credential-stuffing are typically tied to the fact many users reuse the same credentials on multiple accounts.

"This collection can be easily be turned into a single list of emails and passwords: and then all that attackers need to do is to write a relatively simple software program to check if the passwords are working," said Lozhkin.

From there, attackers can wreak all kind of havoc. "The consequences of account access can range from very productive phishing, as criminals can automatically send malicious e-mails to a victim's list of contacts, to targeted attacks designed to steal victims' entire digital identity or money or to compromise their social media network data," said Lozhkin.

It's not unusual for these kinds of data dumps to go unnoticed for a length of time; overall, it takes an average of 15 months for a credential breach to be reported, according to Shape Security..

"Half of all credential spills were discovered and reported within the first four months of the compromise. However, because some spills take years to discover. It took an average of 15 months between the day that an attacker accessed the credentials to the day the spill was reported in 2017," according to a report from Shape Security on credential breaches.

The Threat to Businesses

Credential-stuffing attacks are often aimed at one service or company, as was the case with Dunkin Donuts back in November.

"Massive data breaches like Collection #1 create huge spikes in bot traffic on the login screens of websites, as hackers cycle through enormous lists of stolen passwords," said Distil co-founder Rami Essaid, via email. "While this is often framed as a problem for the individuals who own the passwords, any online business that has a user login web page is at risk of becoming the next breach headline."

Aside from the consumer impact, these kinds of attacks also affect businesses, he added. In May 2018, the Distil Research Lab conducted a study of 600 website domains that include login pages, which found that after the credentials from a data breach have been made publicly available, websites experience a 300 percent increase in volumetric attacks. In the days following a public breach, websites experience three times more credential stuffing attacks than the average of two to three attacks per month.

"Password dumps create a ripple effect of organizations spending precious time and resources on damage control," Essaid explained. "The massive spike in failed logins, then the access into someone else's account before the hacker changes the password, then the account lock-out for the real user, then the customer service calls to regain access to their account. All because a username and password was stolen from a different website."

The potential losses tied to credential spills is $50 million a day globally, Shape Security said.

> ***Note from the Bulletin's authors: The data breach has also affected multiple websites in Bulgaria as identified by our Advanced Security Operations Center analysts.***

Source: https://threatpost.com/773m-credentials-dark-web/

2. EU Offers Bug Bounties For 14 Open Source Projects

The European Commission in January is funding 14 bug bounty programs in hopes of sniffing out vulnerabilities in the free open source projects that EU institutions rely on. The bug bounty programs span 14 open source software projects and offers a total of almost $1 million for all bounties combined. The bug bounty programs have varying rewards, start and end dates, and platforms. The first bug bounty programs – for Filezilla, Apache Kafka, Notepad++, PuTTy, and VLC Media Player – begin next week on Jan. 7.

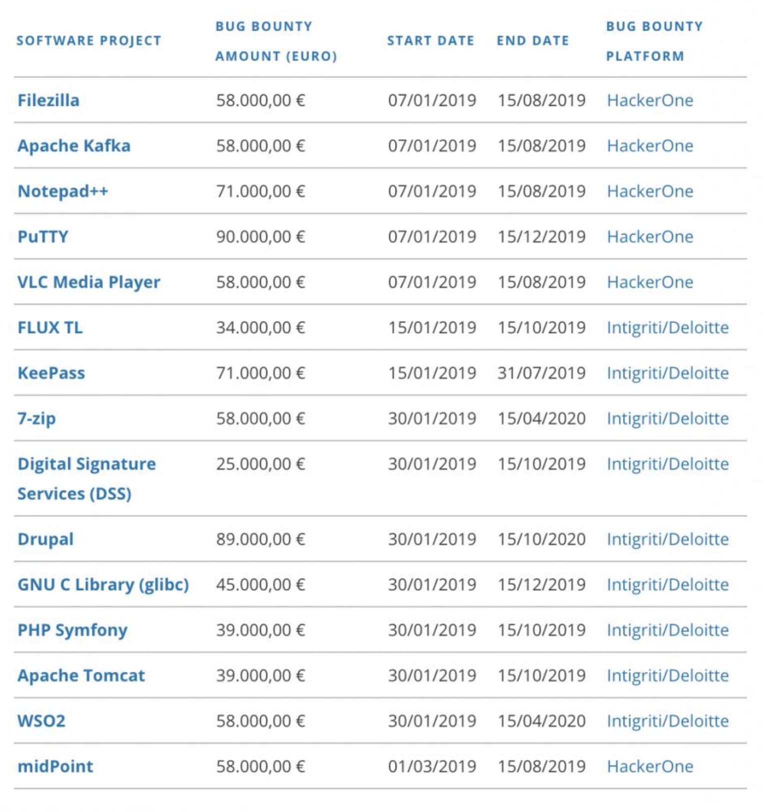
The initiative stems back to the Free and Open Source Software Audit project (FOSSA), first created by European Parliament member Julia Reda. Reda proposed FOSSA with the hopes of securing open source software, after the Heartbleed vulnerability was discovered in open source encryption library OpenSSL in 2014.

Heartbleed not only impacted OpenSSL, but also the other software that the library provided functions to – and the bug also highlighted the security issues in software widely used across the Commission.

“Like many other organisations, institutions like the European Parliament, the Council and the Commission build upon Free Software to run their websites and many other things,” said Reda in a post about FOSSA. “But the Internet is not only crucial to our economy and our administration. It is the infrastructure that runs our every day lives. It is the means we use to retrieve information and to be politically active.”

The project’s first iteration, between 2015 to 2016, launched several security audits, listed which free software the EU runs on, and analyzed how software developers maintain security in their projects. In 2017, the EU developed several bug bounty programs to hunt out vulnerabilities in the open source programs utilized by EU institutions. In November 2017, the Commission announced to run the first bug bounty on VLC Media Player as a proof of concept.

Here is the full list of software projects that will have bug bounty programs:



SOFTWARE PROJECT	BUG BOUNTY AMOUNT (EURO)	START DATE	END DATE	BUG BOUNTY PLATFORM
Filezilla	58.000,00 €	07/01/2019	15/08/2019	HackerOne
Apache Kafka	58.000,00 €	07/01/2019	15/08/2019	HackerOne
Notepad++	71.000,00 €	07/01/2019	15/08/2019	HackerOne
PuTTY	90.000,00 €	07/01/2019	15/12/2019	HackerOne
VLC Media Player	58.000,00 €	07/01/2019	15/08/2019	HackerOne
FLUX TL	34.000,00 €	15/01/2019	15/10/2019	Intigriti/Deloitte
KeePass	71.000,00 €	15/01/2019	31/07/2019	Intigriti/Deloitte
7-zip	58.000,00 €	30/01/2019	15/04/2020	Intigriti/Deloitte
Digital Signature Services (DSS)	25.000,00 €	30/01/2019	15/10/2019	Intigriti/Deloitte
Drupal	89.000,00 €	30/01/2019	15/10/2020	Intigriti/Deloitte
GNU C Library (glibc)	45.000,00 €	30/01/2019	15/12/2019	Intigriti/Deloitte
PHP Symfony	39.000,00 €	30/01/2019	15/10/2019	Intigriti/Deloitte
Apache Tomcat	39.000,00 €	30/01/2019	15/10/2019	Intigriti/Deloitte
WSO2	58.000,00 €	30/01/2019	15/04/2020	Intigriti/Deloitte
midPoint	58.000,00 €	01/03/2019	15/08/2019	HackerOne

PuTTY and Drupal have the two largest bug bounties, offering 90,000 Euro ($102,000) and 89,000 Euro ($101,000) respectively. The timeframes of the bug bounties also vary – PuTTY’s bug bounty program will remain active until Dec. 15, while Drupal’s will go until Oct. 15, 2020.

Lingering Concerns

While the EU hailed the bug bounty programs as a step in the right direction, some worry that open source software needs to rely on more than merely bug bounty programs to build up security.

Katie Moussouris, founder of Luta Security, said on Twitter that "a #bugbounty on open source projects that don't get any funding for additional maintainers is likely to decimate the volunteer maintainer labor pipeline of the future".

The issue of using bug bounty programs as a final solution when it comes to security – as opposed to as a means to an end – has been touched on several times in the past few years.

Josh Bressers, head of Product Security at Elastic, said in his blog one issue is that the EU doesn't have a way to pay the projects today, but they do have a way to pay security bug bounties. They instead should be focusing on a "next step" that will give the projects resources to secure themselves.

"If nothing changes and bug bounties are the only way to spend money on open source, this will fizzle out as there isn't going to be a massive return on investment," he said. "The projects are already overworked, they don't need a bunch of new bugs to fix...Resources aren't always money, sometimes it's help, sometimes it's gear, sometimes it's pizza. An organization like the EU has money, they need help turning that into something useful to an open source project."

Source: https://threatpost.com/eu-offers-bug-bounties-for-14-open-source-projects/

3. New Phishing Tactic Uses Custom Web Fonts to Prevent Detection

Threat actors in the phishing business have adopted a new technique to obfuscate the source code for the forged page by using a custom web font to implement a substitution cipher that looks like plaintext.

When browsers render the phishing page, what users see is the fake landing page created to steal login credentials, as intended by its author.

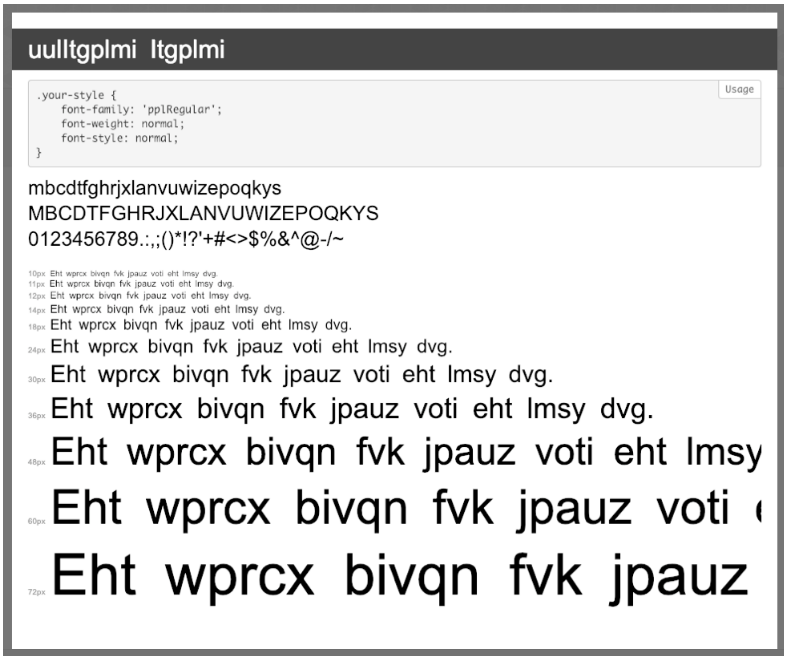
The source code, however, reveals encoded text that makes it difficult to figure out what it does. This is typically implemented through JavaScript functions.

CSS code to do the job

Using a character substitution cipher to avoid detection is not a new tactic, and reversing the text to its original form is not a challenge for automated systems.

The novelty factor here is that the page source did not have JavaScript functions to carry out the substitution, and this was done from the CSS code for the landing page.

The threat actor used only two fonts, 'woff' and 'woff2,' both hidden via base64 encoding.



uulltgplmi ltgplmi

```
.your-style {
    font-family: 'pplRegular';
    font-weight: normal;
    font-style: normal;
}
```

mbcdtfghrjxlanvuwizepoqkys
MBCDTFGHRJXLANVUWIZEPOQKYS
0123456789.:,;()*!?'+#<>$%&^@-/~

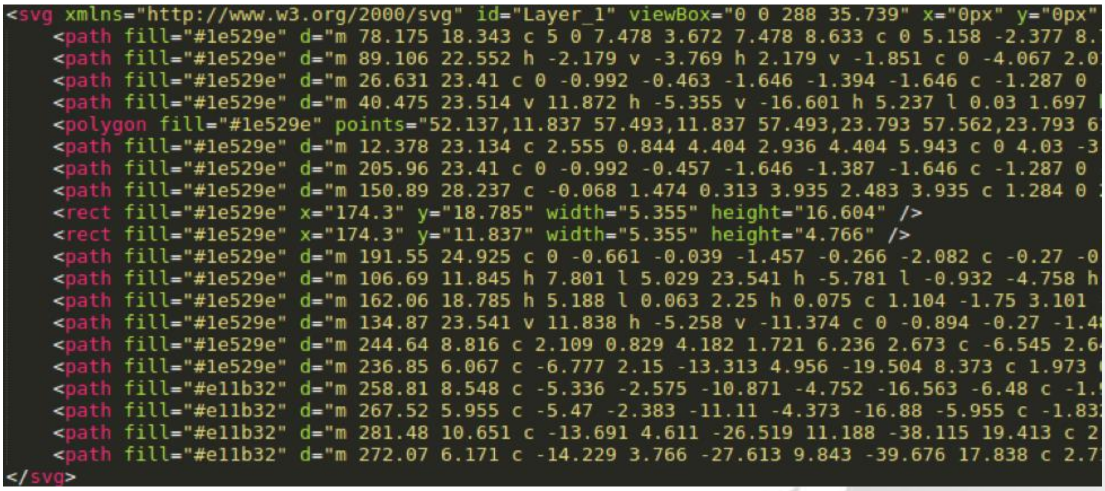
10px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
11px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
12px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
14px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
18px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
24px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
30px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
36px Eht wprcx bivqn fvk jpauz voti eht lmsy dvg.
48px Eht wprcx bivqn fvk jpauz voti eht lmsy
60px Eht wprcx bivqn fvk jpauz voti
72px Eht wprcx bivqn fvk jpauz

Picture 1. woff font specification

Researchers were able to determine that the phishing page has a custom web font file that enables the web browser to render the ciphertext as plaintext.

"As the Web Open Font Format (WOFF) expects the font to be in a standard alphabetical order, replacing the expected letters "abcdefghi..." with the letters to be substituted, the intended text will be shown in the browser, but will not exist on the page," Proofpoint malware analysts explain in a blog post.

To further obfuscate the phishing attempt, the threat actor used branding imagery in SVG (scalable vector graphics) format, which can be rendered through code, eliminating the need to load them from a location that stores image resources, which would help with detection.



```
<svg xmlns="http://www.w3.org/2000/svg" id="Layer_1" viewBox="0 0 288 35.739" x="0px" y="0px"
    <path fill="#1e529e" d="m 78.175 18.343 c 5 0 7.478 3.672 7.478 8.633 c 0 5.158 -2.377 8.
    <path fill="#1e529e" d="m 89.106 22.552 h -2.179 v -3.769 h 2.179 v -1.851 c 0 -4.067 2.0
    <path fill="#1e529e" d="m 26.631 23.41 c 0 -0.992 -0.463 -1.646 -1.394 -1.646 c -1.287 0
    <path fill="#1e529e" d="m 40.475 23.514 v 11.872 h -5.355 v -16.601 h 5.237 l 0.03 1.697
    <polygon fill="#1e529e" points="52.137,11.837 57.493,11.837 57.493,23.793 57.562,23.793 6
    <path fill="#1e529e" d="m 12.378 23.134 c 2.555 0.844 4.404 2.936 4.404 5.943 c 0 4.03 -3
    <path fill="#1e529e" d="m 205.96 23.41 c 0 -0.992 -0.457 -1.646 -1.387 -1.646 c -1.287 0
    <path fill="#1e529e" d="m 150.89 28.237 c -0.068 1.474 0.313 3.935 2.483 3.935 c 1.284 0
    <rect fill="#1e529e" x="174.3" y="18.785" width="5.355" height="16.604" />
    <rect fill="#1e529e" x="174.3" y="11.837" width="5.355" height="4.766" />
    <path fill="#1e529e" d="m 191.55 24.925 c 0 -0.661 -0.039 -1.457 -0.266 -2.082 c -0.27 -0
    <path fill="#1e529e" d="m 106.69 11.845 h 7.801 l 5.029 23.541 h -5.781 l -0.932 -4.758 h
    <path fill="#1e529e" d="m 162.06 18.785 h 5.188 l 0.063 2.25 h 0.075 c 1.104 -1.75 3.101
    <path fill="#1e529e" d="m 134.87 23.541 v 11.838 h -5.258 v -11.374 c 0 -0.894 -0.27 -1.4
    <path fill="#1e529e" d="m 244.64 8.816 c 2.109 0.829 4.182 1.721 6.236 2.673 c -6.545 2.6
    <path fill="#1e529e" d="m 236.85 6.067 c -6.777 2.15 -13.313 4.956 -19.504 8.373 c 1.973
    <path fill="#e11b32" d="m 258.81 8.548 c -5.336 -2.575 -10.871 -4.752 -16.563 -6.48 c -1.
    <path fill="#e11b32" d="m 267.52 5.955 c -5.47 -2.383 -11.11 -4.373 -16.88 -5.955 c -1.83
    <path fill="#e11b32" d="m 281.48 10.651 c -13.691 4.611 -26.519 11.188 -38.115 19.413 c 2
    <path fill="#e11b32" d="m 272.07 6.171 c -14.229 3.766 -27.613 9.843 -39.676 17.838 c 2.7
</svg>
```

Picture 2. code for SVG imagery

Method used in the wild since at least mid-2018

The new evasion approach has been spotted in a phishing kit with most of its resource files dated early June 2018, but malware researchers first observed it a month earlier.

Given the evasion method used, it is possible that the malicious framework was used in the wild even earlier than this point in time.

Proofpoint experts say that the malicious kit was used in a credential harvesting scheme targeting a major retail bank in the US.

"While encoded source code and various obfuscation mechanisms have been well documented in phishing kits, this technique appears to be unique for the time being in its use of web fonts to implement the encoding," note the researchers.

Source: https://www.bleepingcomputer.com/news/security/new-phishing-tactic-uses-custom-web-fonts-to-prevent-detection/

4. 5.25 Million Unencrypted Passport Numbers Accessed in Starwood Breach

In November 2018, Marriott announced a data breach where there was unauthorized access to their Starwood Preferred Guest reservation system and that the data for up to 500 million guests had been compromised. In an update today, Marriott has stated that the amount of affected customers is lower than expected at 383 million, but that 5.25 million unencrypted password numbers were accessed.

When the breach was first announced, Marriott had stated that there was unauthorized access to the Starwood reservation database since 2014 and that these third-parties had access to data such as passport numbers, Starwood Preferred Guest (SPG) account details, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

In an update released today, Marriott has stated that the total amount of affected victims is less than originally thought.

"Working closely with its internal and external forensics and analytics investigation team, Marriott determined that the total number of guest records involved in this incident is less than the initial disclosure," Marriott stated in their update. "Also, the number of payment cards and passport numbers involved is a relatively small percentage of the overall total records involved."

This security incident update revealed that the total amount of affected users had an upper limit of 383 million users rather than the original 500 million. They have also stated that approximately 5.25 million unencrypted passport numbers and 20.3 million encrypted password numbers were accessed. There is no evidence at this time that the hacker was able to access the master decryption key for the encrypted numbers.

The update also states that 8.6 million encrypted payment cards were accessed, with approximately 354,000 payment cards being unexpired as of September 2018. They go on to say that there is no evidence that the third-parties had access to the key to decrypt these payment cards. As a precaution, though, they are searching through other fields in the database to make sure unencrypted payment information is not stored in them.

For those who were affected by this breach, Marriott has a dedicated support site at https://answers.kroll.com/ where users can sign up for a free web monitoring service and phone numbers that can be called for more information. They have also stated that customers can contact the listed phone numbers in order to receive a method to check if your passport numbers was one of the ones that was stored unencrypted in the database.

Finally, the original Starwood reservation database is now shutdown as part of their merger with Marriott. All reservations are now going through the Marriott reservation system.

Source: https://www.bleepingcomputer.com/news/security/525-million-unencrypted-passport-numbers-a3ccessed-in-starwood-breach/

5. Deciphering the Encryption Paradox

As security professionals, we all understand the importance of protecting data and the need for proper encryption. It’s no surprise, then, that more and more traffic crossing our networks is encrypted. This is a good thing from both a security and privacy perspective, but what if the encryption is being used to hide malicious activity on enterprise networks?

When Encryption Works Against Security

Our networks not only facilitate the connected world in which our businesses thrive, but also provide the conduit for threats to infiltrate our organizations. Threat activity can easily hide deep within network content to avoid detection by traditional methods, which is why we need solutions that can analyze this content with application-level context to distinguish legitimate activity from malicious behavior. But what happens when our network data is encrypted?

Here’s the irony: As more and more network traffic is encrypted, we’re gaining more and more options to decrypt that data. I know it sounds counterintuitive, but as more network traffic is encrypted, there is an increasing need for network vendors to build decryption capabilities into their devices.

Since many of these devices are already deployed inline, they can terminate an encrypted session on one side and start another encrypted session on the other. The data remains encrypted in transit on both sides of the network device, but it provides visibility into the traffic in its decrypted form. Whether it’s a next-generation firewall looking to block intruders or a managed switch directing or filtering select data, visibility is key.

Many of these devices allow decrypted traffic to be mirrored out of a port for full content analysis. As a result, most organizations have either deployed or plan to deploy network devices that are capable of decrypting traffic. Gaining the network visibility we need to secure our organizations is often a matter of enabling those decryption capabilities.

To Decrypt, or Not to Decrypt …

While network visibility is crucial for identifying malicious activity as it crosses a network, there are cases where we may prefer to keep that data encrypted at all times. But despite our best efforts, it's often difficult to ensure that all of our sensitive data is encrypted properly. Just think of the myriad devices and applications that need to be configured properly to encrypt communications with the latest protocol versions.

By analyzing every network session in detail and knowing which are encrypted, how strong the certificates are, and what encryption protocol version is in use, we can ensure that our data is adequately protected. And while it's tempting to focus on reports that the volume of encrypted web traffic is increasing, it's easy to forget about the large amount of traffic on our networks that is associated with non-web applications spanning a wide range of network protocols. Many organizations find that when they take a deeper look into the data that is crossing their networks, a lot less is encrypted than originally thought.

Clearly, we are trending toward increased encryption of network data and we should all embrace it as a valuable tool to help protect our crown jewels. But it's not the roadblock many think it is when it comes to deep network analysis. There is a growing variety of methods and devices that deliver full network content visibility in a controlled and secure manner. Every organization should consider this approach as part of its network and security evolution and strategy.

Source: https://securityintelligence.com/deciphering-the-encryption-paradox/

6. U.S. Government Shutdown Leaves Dozens of .Gov Websites Vulnerable

As the U.S. federal shutdown continues, dozens of U.S. government websites have been rendered either insecure or inaccessible due to expired transport layer security (TLS) certificates that have not been renewed.

In fact, .gov websites are using more than 80 TLS certificates that have expired, according to a new Thursday report by Netcraft. That's because funding for renewals has been paused. That opens the impacted sites to an array of cyber-attacks; most notably, man-in the-middle attacks, which allow bad actors to intercept exchanges between a user and a web application—either to eavesdrop or to impersonate the website and steal any data that the user may input.

Dozens of sites are impacted, which include sensitive government payment portals and remote access services for organizations like NASA, the U.S. Department of Justice and the Court of Appeals.

The security issue has raised alarms as the U.S. government continues to be crippled by a partial government shutdown, which as of Friday has been ongoing for 21 days. About

800,000 federal employees are furloughed or temporarily working without pay, and millions more government contractors have been told not to come to work.

"With Donald Trump seemingly unwilling to compromise on his demands for a wall along the border with Mexico, and Democrats refusing to approve a budget containing $5.7B for the wall, the hundreds of thousands of unpaid federal employees might not be the only ones hurting," said Netcraft. "As more and more certificates used by government websites inevitably expire over the following days, weeks — or maybe even months — there could be some realistic opportunities to undermine the security of all U.S. citizens."

One impacted U.S. website, belonging to the Department of Justice, uses a certificate that expired in the week leading up the shutdown. According to Netcraft, the certificate was signed by trusted certificate authority GoDaddy – but it has not been renewed since it expired on December 17.

Another, the .gov website for Berkeley Lab, expired on January 8 and has not yet been replaced.

The issue has sparked concerns in the infosec space about how the sensitive government websites can be abused – and what other security issues are raised due to the shutdown.

"How many critical governmental systems are currently unmaintained, outdated and thus vulnerable? It seems to be a great opportunity for nation-state hacking groups to exploit U.S.' momentary weakness to steal or alter extremely sensitive information," High-Tech Bridge's CEO Ilia Kolochenko said in an email.

HSTS Policies

Luckily, certain security measures were implemented before the shutdown that protects some .gov websites from cyber-attacks when their certificates have expired – but the downside is that those protected websites can no longer be accessed.

The security measure puts certain usdoj.gov domains and any subdomains that are on Chromium's HSTS preload list, which is a list of sites hard-coded into Chrome as being HTTPS only. This security measure prevents users from visiting the HTTPS sites when they have an expired certificate.

However, not all sites implement the HSTS policies, and "consequently, most of the affected sites will display an interstitial security warning that the user will be able to bypass," Netcraft said. While that means that the websites can at least be accessed, "this introduces some realistic security concerns, as task-oriented users are more likely to ignore these security warnings, and will therefore render themselves vulnerable to man-in-the-middle attacks."

Gov Shutdown's Impact on Security

As the government shutdown continues, it has an array of impacts across the board when it comes to security.

Fortalice Solutions' Theresa Payton, the former White House CIO, said that the shutdown has an array of implications for cybersecurity issues across the country, including short-staffing agencies that are working on cybersecurity, spooking cybersecurity professionals who might otherwise be interested in public service or government contracting, and interfering with timelines for contracts.

"Leaders and legislators on both sides of the aisle would do well to take an 'all-of-the-above' approach when it comes to this shutdown and our national security goals," she told Threatpost.

Kolochenko meanwhile said that moving forward, an emergency plan needs to be developed to deal with continuing critical security measures even during a government shutdown.

"The situation… points to a continuity plan that is poorly implemented in some federal agencies: Critical cybersecurity tasks and processes have to be maintained even if financing is temporarily paused," Kolochenko said. "Otherwise, the entire model of governmental cybersecurity is questionable, and people may reasonably inquire where do their taxes go."

Source: https://threatpost.com/u-s-government-shutdown-leaves-dozens-of-gov-websites-vulnerable/

7. ThreatList: $1.7M is the Average Cost of a Cyber-Attack

The average cost estimate for cleaning up a cyberattack comes in at around $1.1 million, according to a recent survey. But this is actually a rosy view: For those organizations that actually calculate (versus estimate) the real cost of an attack, that number increases significantly to $1.67 million.

According to Radware's 2018-2019 Global Application and Network Security Report, which analyzed vendor-neutral survey data from 790 IT executives, there has been a 50 percent growth in organizations that estimate the cost of an attack to be greater than $1 million, and an overall shift away from lower estimations.

"Quantifiable monetary losses can be directly tied to the aftermath of cyberattacks in lost revenue, unexpected budget expenditures and drops in stock values," according to the report. "Protracted repercussions are most likely to emerge as a result of negative customer experiences, damage to brand reputation and loss of customers."

About half of the respondents said that the main impact of an attack lies in revenue-killing operational and productivity loss (54 percent), followed by negative customer experience (43 percent).

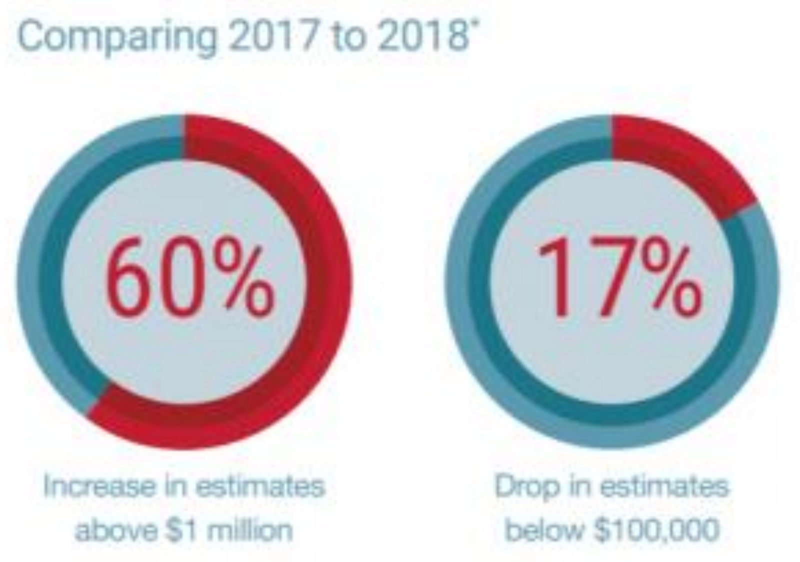


Figure 22. Companies' estimates of costs related to cyberattacks are on the rise.
*Companies surveyed in both years were of similar size and revenues.

Picture 3. increasing cost of cyber attacks

And no wonder: The majority (78 percent) of respondents hit by a cyberattack said they experienced service degradation or a complete outage (almost half, 45 percent, reported that the goal of the attacks they suffered was to cause just that). The situation is worsening, too: 68 percent last year said an attack led to service interruption.

Data leakage and information loss remain the biggest concern to more than one-third (35 percent) of businesses, followed by service outages. This dovetails with the fact that for a third of responding victims (35 percent), the goal of the attack was data theft.

While the cost of attack mitigation continues to rise, so does the number of organizations under attack. Most organizations have experienced some type of attack within the course of a year, with only 7 percent of respondents claiming not to have experienced an attack at all. A fifth (21 percent) reported daily attacks, representing a significant rise from 13 percent last year. And yet, a third (34 percent) said they don’t have a cybersecurity emergency response plan in place.

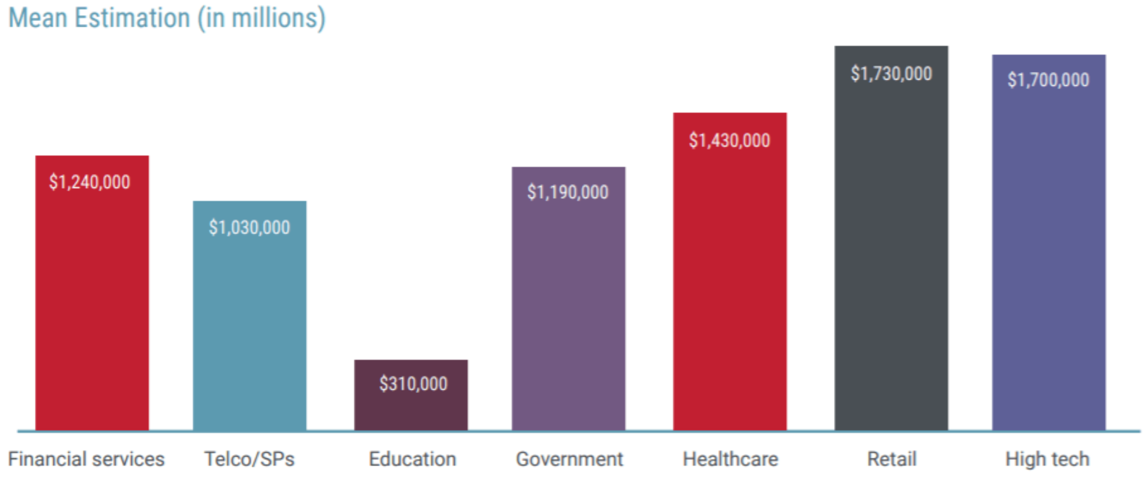
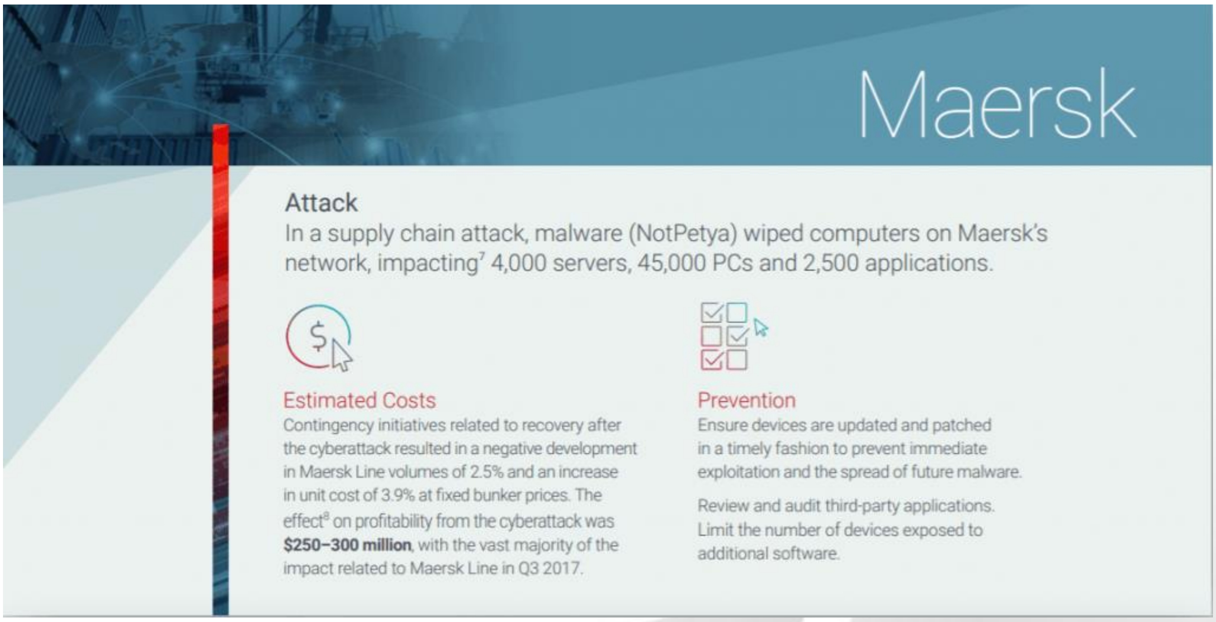


Figure 24. Estimated cost related to cyberattacks by vertical market.

Figure 4. Estimated cost related to cyberattacks by vertical market

"While threat actors only have to be successful once, organizations must be successful in their attack mitigation 100 percent of the time," said Anna Convery-Pelletier, CMO for Radware, in the report. "A cyberattack resulting in service disruption or a breach can have devastating business impacts. In either case, you are left with an erosion of trust between a brand and its constituency."

In terms of threat scenarios, malefactors increased their usage of emerging attack vectors to bring down networks and data centers: Respondents reporting HTTPS floods grew from 28 percent to 34 percent; reports of DNS attacks grew from 33 percent to 38 percent; reports of burst attacks grew from 42 percent to 49 percent; and reports of bot attacks grew from 69 percent to 76 percent.



Maersk

Attack

In a supply chain attack, malware (NotPetya) wiped computers on Maersk's network, impacting[7] 4,000 servers, 45,000 PCs and 2,500 applications.

Estimated Costs

Contingency initiatives related to recovery after the cyberattack resulted in a negative development in Maersk Line volumes of 2.5% and an increase in unit cost of 3.9% at fixed bunker prices. The effect[8] on profitability from the cyberattack was **$250–300 million**, with the vast majority of the impact related to Maersk Line in Q3 2017.

Prevention

Ensure devices are updated and patched in a timely fashion to prevent immediate exploitation and the spread of future malware.

Review and audit third-party applications. Limit the number of devices exposed to additional software.

Application-layer attacks meanwhile still cause considerable damage. Two-thirds of respondents experienced DoS attacks against specific services, and 34 percent foresee application vulnerabilities being a major concern in the coming year. More than half (56 percent) reported making changes and updates to their public-facing applications monthly, while the rest made updates more frequently – opening the door to misconfiguration or the introduction of weaknesses.

Source: https://threatpost.com/threatlist-cost-cyber-attack/

8. Banks in West Africa Hit with Off-The-Shelf Malware, Free Tools

Attacks hitting financial organizations in West Africa since at least mid-2017 rely on off-the-shelf malware, free hacking tools, and utilities already available on the target systems to steal credentials, install backdoors, and run commands.

Researchers observed four attack campaigns targeting institutions in Cameroon, Congo (DR), Ghana, Equatorial Guinea, and Ivory Coast. Some of the tools used cost as little as $25, although the use of the more expensive commercial penetration testing tool Cobalt Strike was also observed.

NanoCore trojan and PsExec

In one of the attacks, the threat actor used NanoCore trojan along with PsExec, a legitimate network administration tool, and delivered the malware via phishing emails.

Researchers part of Symantec's Targeted Attacks Investigation Team say that this attack has been underway since at least mid-2017.To lure the victim into installing the malware, the attacker used documents referring to a West African bank. The targets were in Ivory Coast and Equatorial Guinea.

The author of NanoCore was arrested in early 2017 and sentenced to 33 months in prison and two years of supervised release. He advertised the remote access trojan (RAT) on a hacker forum between 2014 and 2016 and then sold it to an unknown party.

Cobalt Strike, PowerShell scripts, and free tools

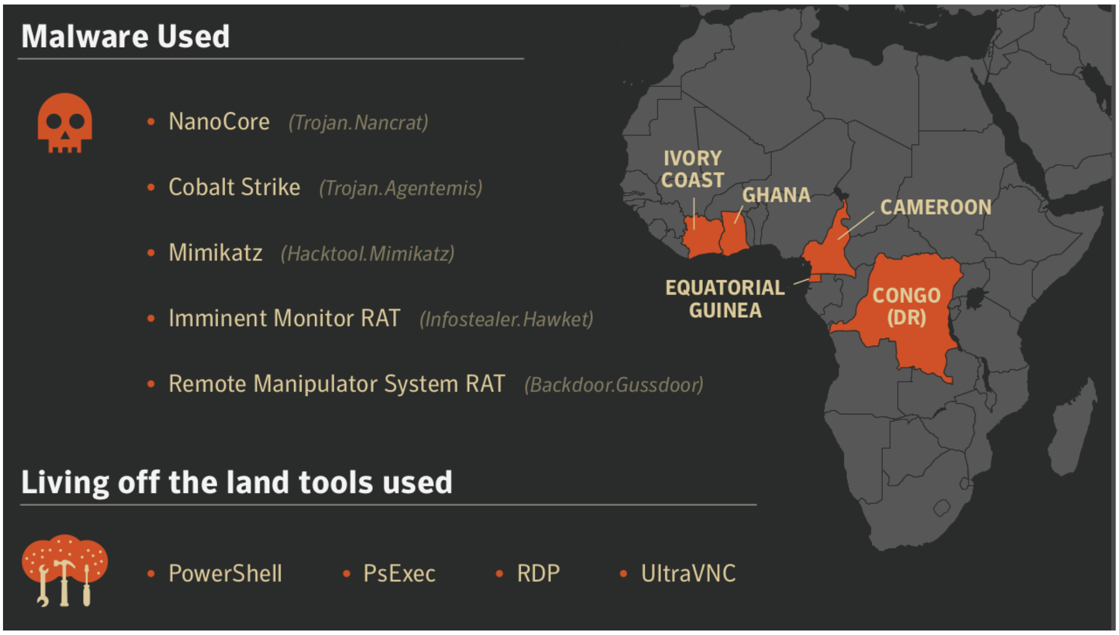
Another attack began in late 2017 and hit victims in Ivory Coast, Ghana, Congo (DR), and Cameroon. It combined malicious PowerShell scripts with Mimikatz, a hacking tool designed to steal credentials, and UltraVNC open-source software for remote administration. The researchers say that Cobalt Strike was also employed to set a backdoor on the compromised system and to communicate with a command and control (C2) server. The attackers also used a dynamic DNS service to hide their location by assigning a custom domain name to the IP address of the C2 server.

Mimikatz and custom RDP

In a third incident observed by the researchers, the intruders relied on Mimikatz, two custom remote desktop control tools, and the Remote Manipulator System (RMS) RAT.

"Since Mimikatz can be used to harvest credentials and RDP allows for remote connections to computers, it’s likely the attackers wanted additional remote access capability and were interested in moving laterally across the victim’s network," say the researchers in a report shared with BleepingComputer.

A fourth attack started in December 2018 against a target in Ivory Coast and used the Imminent Monitor RAT.



Malware Used

- NanoCore (Trojan.Nancrat)
- Cobalt Strike (Trojan.Agentemis)
- Mimikatz (Hacktool.Mimikatz)
- Imminent Monitor RAT (Infostealer.Hawket)
- Remote Manipulator System RAT (Backdoor.Gussdoor)

Living off the land tools used

- PowerShell
- PsExec
- RDP
- UltraVNC

None of the tools are new

It is worth noting that none of the tools used in these attacks are new or hard to come by. RMS, for instance, was discovered around 2011, while Imminent Monitor RAT is known since 2015. Also, tutorials teaching about how to configure and use them abound on video-sharing websites.

Cobalt Strike is notorious for being used by the Cobalt/Carbanak bank robbers, who use it to build custom malware. The group ran over 100 hacks in more than 40 countries and stole in excess of 1 billion euros.

"A growing number of attackers in recent years are adopting “living off the land” tactics—namely the use of operating system features or network administration tools to compromise victims’ networks. By exploiting these tools, attackers hope to hide in plain sight, since most activity involving these tools is legitimate," Symantec concludes.

Source: https://www.bleepingcomputer.com/news/security/banks-in-west-africa-hit-with-off-the-shelf-malware-free-tools/

9. Google Fined $57M in Largest GDPR Slap Yet

France's National Data Protection Commission (CNIL) has fined Google $57 million (€50 million) for violations of the General Data Protection Regulation (GDPR) – the largest fine yet issued under the EU's new data privacy law.

In investigating group complaints from privacy advocacy groups None Of Your Business and La Quadrature du Net (the latter representing 10,000 citizens), CNIL found Google lacking in transparency when it comes to how it collects and handles user data in the name of serving up personalized ads.

"Despite the measures implemented by Google (documentation and configuration tools), the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life, since they are based on a huge amount of data, a wide variety of services and almost unlimited possible combinations," CNIL said in a Monday statement.

The regulator also noted the scope of the violations' impact.

"The violations are continuous breaches of the Regulation as they are still observed to date. It is not a one-off, time-limited, infringement," it said, adding, "taking into account the important place that the operating system Android has on the French market, thousands of French people create, every day, a Google account when using their smartphone."

GDPR Violations

Under the GDPR, consent must be obtained before any data is collected, let alone kept or used for follow-on purposes, such as targeted advertising. This means information gleaned from websites, account registrations, social media, advertising and marketing efforts, newsletters and list rentals, data brokerages, public sources of information and more.

This profoundly changes the way an American company, such as Google's subsidiary DoubleClick, profiles and targets ads to internet users in the E.U.

In this case, the French regulator determined that information from Google about how data is collected, collated and used across as many as 20 different Google services is relatively obscured. The internet giant, according to CNIL, breaks up the information across several documents, so that the full extent of Google's data processing practices can only be uncovered by going down a rabbit hole of several links.

"The relevant information is accessible after several steps only, implying sometimes up to five or six actions," CNIL said on Monday in its statement. "For instance, this is the case when a user wants to have complete information on his or her data collected for the personalization purposes or for the geo-tracking service."

Further, even after accessing the pertinent information, the documents lack detail in terms of exactly where and how user data is utilized for advertising purposes, according to CNIL.

"The [data] processing operations are particularly massive and intrusive because of the number of services offered (about 20), [and] the amount and the nature of the data [being] processed and combined," the regulator explained. Google's practices are "described in a too generic and vague manner, and so are the categories of data processed for these various purposes."

As such, CNIL determined that Google doesn't obtain valid consent from users to use their data for ad personalization – explicit consent being a key requirement of the GDPR.

"The users' consent is not sufficiently informed…[because the information] is diluted in several documents and does not enable the user to be aware of their extent," the authority noted. Thus, "the collected consent is neither 'specific' nor 'unambiguous.'"

CNIL added that even though users can modify their account options to opt out of seeing personalized ads, the option to see them is pre-ticked, meaning there is no "clear affirmative action from the user (by ticking a non-pre-ticked box for instance)" to receive the ads.

And finally, before creating an account, the user is asked to tick a box for "I agree to Google's Terms of Service" and "I agree to the processing of my information as described above and further explained in the Privacy Policy." However, CNIL said this isn't specific and matched to a distinct purpose, and therefore does not satisfy GDPR rules.

GDPR Enforcement Ramps Up

The Google fine is far and away the largest penalty issued since the GDPR went into effect last May. However, it could have been much larger: GDPR violations can incur fines of up to 4 percent of global turnover.

While the GDPR is a European regulation, it affects any organization that handles data on E.U. citizens, whether they be customers or partners – including American companies. That means any entity in the U.S. is subject to enforcement actions, such as fines, if they do business with any E.U. citizen. In other words, it's an E.U. law, but has global applicability.

Enforcement actions have been slow to roll out, largely because it takes time to build a consensus on how to determine compliance. The GDPR contains a series of articles that lay out a complex set of requirements for those handling E.U. citizen data. Yet, in terms of what compliance actually looks like in the real world, there are several areas of uncertainty that will only play out and become clarified over time.

Google is the largest fish to be caught in the GDPR net to date, but it surely won't be the last. Over the course of the fall, Data Protection Authorities (DPAs) in various countries began leaping into the enforcement fray – a state of affairs that's unlikely to wane anytime soon.

Some of the actions have not carried fines: The U.K.'s Information Commissioner's Office (ICO) for instance in October found that Canada-based AggregateIQ Data Services used personal data—including names and email addresses—of U.K. individuals to target them with political advertising messages on social media without their consent. The ICO ordered AggregateIQ to erase any personal data of U.K. individuals retained on its servers.

Similarly, in France, CNIL recently found that a mobile marketing and ad tech agency, Vectuary, illegally obtained the consent of more than 67 million people to collect their data. It was also ordered to purge all personal data for the affected individuals.

On the financial penalty front, in September Austria's Osterreichische Datenschutzbehorde fined a retailer €4,800 for using a surveillance camera that recorded passersby without their consent. Also, Portugal's Comissao Nacional de Proteccao de Dados fined a hospital, Barreiro Montijo, €400,000 for not restricting employee access to patient data.

Most recently, Germany's State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg fined a German social-media company and maker of the flirting app "Knuddels" €20,000 in November after a data breach. It came to light that the service was storing user passwords in plain text, without pseudonymizing and encrypting personal data as required by the GDPR.

Source: https://threatpost.com/google-fine-privacy-gdpr/

10. U.S. Gov Issues Urgent Warning of DNS Hijacking Attacks

The Department of Homeland Security is ordering all federal agencies to urgently audit Domain Name System (DNS) security for their domains in the next 10 business days.

The department's rare "emergency directive," issued Tuesday, warned that multiple government domains have been targeted by DNS hijacking attacks, allowing attackers to redirect and intercept web and mail traffic.

"[The Cybersecurity and Infrastructure Security Agency] (CISA) is aware of multiple executive branch agency domains that were impacted by the tampering campaign and has notified the agencies that maintain them," said the alert.

The warning comes on the heels of a Jan. 10 FireEye report which detailed a wave of DNS hijacking attacks targeting victims in North America, Europe, Middle East and North Africa.

The Attacks

DNS hijacking is a type of malicious attack in which an individual redirects queries to a domain name server via overriding a computer's transmission control protocol/internet protocol (TCP/IP) settings – generally by modifying a server's settings.

The DHS, for its part, said that the attacker begins by logging into the DNS provider's administration panel using previously-compromised credentials.

The attacker then alters DNS records – including the address mail exchanger or name server records – and replaces the legitimate address of a service with their own address controls, thus redirecting traffic. Attackers can also alter and tamper with the traffic flows.

“This enables them to direct user traffic to their own infrastructure for manipulation or inspection before passing it on to the legitimate service, should they choose,” said the DHS in its advisory. “This creates a risk that persists beyond the period of traffic redirection.”

Since the attackers can set record values for the domain name systems, they can obtain valid encryption certificates for an organization’s domain names; this allows browsers to establish a connection without any certificate errors as the certificate can be trusted, FireEye researchers said. In the most recent campaigns, the attackers have used certificates from the Let’s Encrypt open certificate authority.

That valid certificate then enables the redirected traffic to be decrypted and exposes any user-submitted data.

Government Response

The emergency directive issued by the DHS provides “required actions” that government agencies must fulfill in the next 10 business days.

“To address the significant and imminent risks to agency information and information systems presented by this activity, this emergency directive requires… near-term actions to mitigate risks from undiscovered tampering, enable agencies to prevent illegitimate DNS activity for their domains and detect unauthorized certificates,” said the report.

First, the DHS said all .gov domain admins must audit their DNS records over the next 10 days to verify if any traffic is being redirected.

The department also urged agencies to update their passwords for all accounts on systems that can make changes to agency DNS records, and to implement multi-factor authentication for accounts on DNS admin systems. Finally, agencies are being directed to monitor certificate transparency logs.

The warning comes as the U.S. government enters its 33rd day of a shutdown (as of Wednesday), a longstanding incident which has sparked concerns about its impact across the board when it comes to security.

Iran Attribution

Researchers assess “with moderate confidence” that the recent DNS hijacking activity is conducted by a group or groups in Iran, and that the activity aligns with Iranian government interests.

The attacks have been observed in clusters between January 2017 to January 2019, the researchers said in an analysis of the attacks.

Alister Shepherd, MEA director of Mandiant at FireEye, told Threatpost that the campaign is ongoing – but that there is no indication of how many credentials have been harvested thus far. However, researcher do state that the attackers had “a high degree of success” harvesting targets’ credentials.

This most recent DNS hijacking campaign "showcases the continuing evolution in tactics from Iran-based actors," FireEye researchers stressed. "This is an overview of one set of TTPs that we recently observed affecting multiple entities."

Source: https://threatpost.com/gov-warning-dns-hijacking/

11. GDPR Behind 42K Data Breach Notifications, 255 Investigations

A European Commission Statement says that Data Protection Authorities (DPAs) across Europe received 95,180 complaints regarding the mishandling of personal data and companies reported a record number of 41,502 data breaches since the General Data Protection Regulation (GDPR) was enacted on 25 May 2018.

According to the GDPR provisions, businesses have the obligation to report data breaches to their national DPA in under 72 hours if personal data of European citizens is unlawfully or accidentally disclosed.

Following the **95,180 complaints** introduced by both individuals and organizations mandated by individuals since the enactment of the GDPR, a number of **255 investigations** were initiated by national Data Protection Authorities.

41,502 data breaches reported by companies since 25 May 2018

It is important to mention though that out of those, a couple of dozen GDPR investigations were also initiated outside the scope of the complaints advanced by individuals.

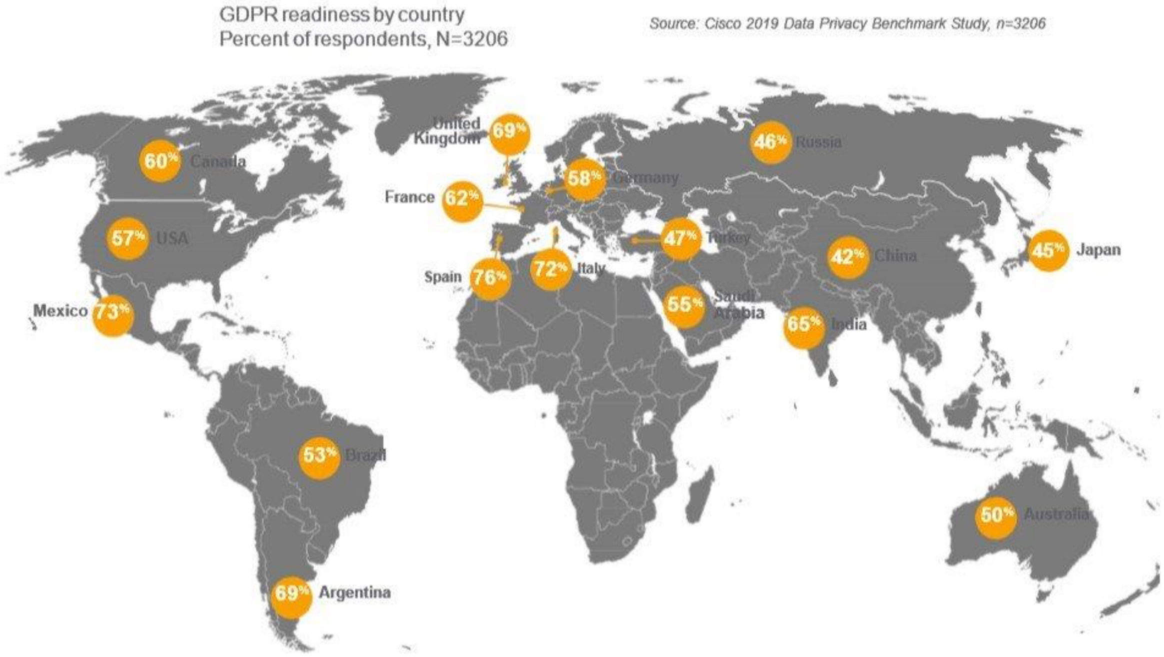
Moreover, European Commission's statistics say that the most common types of GDPR complaints were related to telemarketing, promotional e-mails, and to video surveillance/CCTV, which were found to violate multiple provisions.

European Commission's joint statement said that:

We are already beginning to see the positive effects of the new rules. Citizens have become more conscious of the importance of data protection and of their rights. And they are now exercising these rights, as national Data Protection Authorities see in their daily work. They have by now received more than 95,000 complaints from citizens.

As reported by Cisco in its Data Privacy Benchmark Study, companies which closely follow the requirements of the GDPR experience benefits such as lower frequency and effect of data breaches, as well as shorter downtimes, fewer records being impacted by the attacks, and lower overall costs.

Furthermore, as found out by Cisco, **country GDPR-readiness was between 42% to 76%**, with the European countries involved in the survey (i.e., France, Germany, Italy, Spain, UK) unsurprisingly scoring a lot higher on the scale when compared to countries from other continents.



GDPR readiness by country
Percent of respondents, N=3206

Source: Cisco 2019 Data Privacy Benchmark Study, n=3206

Picture 4. GDPR readiness by country

As an example of GDPR being used to protect the personal data and privacy of European citizens, the Commission Nationale de l'informatique et des Libertés (CNIL) slapped Google with a **€50 million fine** on January 21 for not obtaining user consent for processing data for ads personalization purposes and for violating transparency and information obligations.

Google-owned YouTube is also the target of a GDPR complaint filed by NOYB for "right to access" violations described in GDPR's Article 15, with a **possible maximum penalty that could reach €3.87 Billion** according to the NGO, with Amazon, Apple, DAZN, Spotify, SoundCloud, Flimmit, and Netflix also being targeted by GDPR complaints related to the same reasons.

Acxiom, Oracle, Criteo, Quantcast, Tapad, Equifax, and Experian were also subjects of a GDPR complaint filed by user rights group Privacy International because they were collecting the data of millions to create user profiles.

Source: https://www.bleepingcomputer.com/news/security/gdpr-behind-42k-data-breach-notifications-255-investigations/

12. Phishing Campaign Delivers Nasty Ransomware, Credential-Theft Two-Punch

An array of phishing emails harboring Word attachments with embedded macros have been infecting systems with a deadly malware and ransomware duo.

The campaign, spotted by researchers at Carbon Black, has hit infected systems with a lethal attack combination that harvests credentials, gathers system and process information, and then encrypts data in order to extort payments from victims.

The attack originally came in via phishing emails that contained an attached Word document with embedded macros. The macro would then call an encoded PowerShell script and use a series of techniques to download and execute both a Ursnif malware strain and GandCrab ransomware variant.

The campaign appears to have begun targeting victims on Dec. 17, Carbon Black researchers told Threatpost. There have been a couple of different pockets of activity observed each week since then, they said.

"The campaign appears to be ongoing, as we are seeing additional payloads being posted on pastebin.com that are almost identical to the payloads that were leveraged to data extracted from our analysis of these samples," Jared Myers, senior threat researcher for Carbon Black, told Threatpost.

The Attack

The initial phishing emails included a Microsoft Word document to deliver the early stages of the attack.

"The overall attack leverages several different approaches, which are popular techniques amongst red-teamers, espionage-focused adversaries and large-scale criminal campaigns," said Carbon Black researchers in a Thursday analysis.

These documents contained a VBS macro that, once decompressed, totaled approximately 650 lines of code. Interestingly, the vast majority of that was junk code – and once that was removed, there were about 18 lines of relevant code.

From there, a PowerShell script was downloaded and executed, which then contacted a hard-coded command-and-control (C2) address requesting two strings of code: the DownloadString method, which ultimately downloads the GandCrab ransomware, and the DownloadData method, which eventually downloads the Ursnif malware strain.

GandCrab ransomware has been spotted in several campaigns over the past year, including hidden on legitimate but compromised websites, and infecting victims via a December sextortion campaign.

"The first payload that is downloaded via the DownloadString method…is a PowerShell one-liner that uses an 'if' statement to evaluate the architecture of the compromised system, and then downloads a additional payload from pastebin.com. This additional payload is then executed in memory," researchers said.

The Ursnif executable meanwhile is downloaded from the DownloadData method, and then performs an array of malicious activities like credential harvesting, gathering system and process information, and deploying additional malware samples.

While no additional data is available on the number of victims in the campaign, Carbon Black researchers said that they have located roughly 180 Word document variants in the wild.

“We have not observed where any one particular malicious document was sent at a higher rate to potential victims than any other,” Myers told Threatpost. “However, the variants were presumably created in batches that were then sent to potential victims, so, sepending on the effectiveness of the phishing emails, some may appear to be more successful than others.

Source: https://threatpost.com/phishing-gandcrab-ursnif/

13. Data Privacy Day: What it Means for Your Organization

The US and Canada have observed Data Privacy Day every January 28th since 2008. It is a follow-on to Data Protection Day in Europe that commemorates the Jan. 28, 1981 signing of the Council of Europe treaty known as Convention 108. This treaty was the first legally binding agreement designed to protect an individual's right to digital privacy, anticipating the increasingly automated processing and distribution of personal data.

While remarkably prescient, the original authors and signers of Convention 108 could not have possibly foreseen how data would be being created, shared, processed, and stored today, nor the volume of personal data that exists for virtually every human being on earth.

That original treaty has been enhanced by legally binding legislation over the years in nearly every country in the world, culminating most recently with the most comprehensive law ever enacted to protect personally identifying information (PII). The EU’s General Data Protection Regulation (GDPR) is the most important change to data privacy regulation since that first treaty was signed in 1981. It provides comprehensive data protection and privacy for all individuals within the European Union and the European Economic Area, including the export of personal data outside the EU and EEA.

It has also raised the bar in other countries around the world, with volumes of new legislation patterned after GDPR. The California Consumer Privacy Act of 2018, for example, signed into law in June of 2018, gives California citizens the right to know what personal data businesses possess. As with the EU's GDPR. Californians in 2020 will not only be able to require that organizations delete their PII, but also forbid those organizations from selling their data to third parties. Since California is now the fifth largest economy in the world, surpassing the UK last year, the impact of this new law will have national and international implications.

This past July, two months after the passage of the California law, the White House announced that it was working on a new "consumer privacy protection policy that is the appropriate balance between privacy and prosperity." Since then, members of Congress have introduced multiple data protection bills.

What this means for your organization

If your organization does business with any organizations or individuals in the EU, you have already had to make significant changes to how you process, manage, and store the data of EU residents. Prepare now to provide many of the same sorts of protection to your US and Canadian customers. Here is a quick checklist of the things you will need to do:

- ***Implement a comprehensive, integrated security strategy***. It has been said that there cannot be any data privacy without good data security. Because of that, you have to start by ensuring that any PII data your organization touches is secured from the moment it enters your network to the moment it leaves. This includes applying security measures and policies that can seamlessly identify, follow, and secure data as it moves between network domains and devices, including across multi-cloud or SD-WAN environments, as well as into your storage area network (SAN). Security plays a critical role in helping you know where every bit of data is located and who and what has access to it. An integrated security framework allows all security components to see other devices, share and correlate information between them, and participate in a coordinated threat response. It needs to be woven into and across every aspect of your evolving network to enable things like unified policy creation, centralized orchestration, and consistent enforcement. This approach allows you to extend visibility deep into your infrastructure to see every device, track every application and workflow, and more importantly, see and secure all data. It also allows you to demonstrate compliance with regards to protected privacy requirements and the verification of its secure storage, use, and removal.
- ***Change what and how you collect PII data.*** New privacy laws such as GDPR define individuals as the sole owners of their data, and not businesses or institutions. As a result, these individuals must be able to withdraw their consent to the collection of their data as quickly and easily as it was given. This will require organizations to collect only the minimum amount of data needed for a specific purpose, and to then be able to completely remove it when it is no longer needed.
- ***Reorganize your data so that PII can be easily identified, flagged, and deleted***. Be prepared to demonstrate to compliance officials that you can prevent specific data from being shared or sold to third parties and that you can remove all instantiations of an individual's PII regardless of where it is being stored or used. For larger organizations, this is not a trivial task. It will require significant retooling of databases, rewriting software applications and websites, and redesigning internal processes to simplify and accelerate internal processes to identify all data related to a single customer. The GDPR's "right to be forgotten" (RTBF) means that data needs to be found and removed quickly and easily, rather than relying on humans to hunt for each instance of personal information scattered across your distributed network.
- ***Encrypt PII to ensure that if possesses no risk if compromised***. You should consider encrypting data in transit and at rest in your network. Encryption negates the value of data if it is compromised. But encrypting large volumes of data is no easy task. Organizations should consider ability of encryption performance and any associated degradation of performance.

Summing Up

New and looming data privacy legislation reflects growing public concern about the protection and personal ownership of PII. Data Privacy Day is an urgent reminder that every organization that touches personal data needs to re-evaluate its IT security infrastructure. Are your IT security solutions able to effectively communicate, regardless of where they have been deployed, to optimally protect data and provide network-wide visibility? Does your network include sophisticated data-protection measures such as threat prevention and detection, pseudonymization of PII, and internal segmentation to isolate and track customer and employee data? And finally, have you documented, and more importantly, tested your data-breach response plan?

Today's organizations need to be able to answer "yes" to these questions if they want to be prepared for the new data privacy regulations on the near horizon.

Source: https://www.fortinet.com/blog/industry-trends/data-privacy-day--what-it-means-for-your-organization.html

14. Addressing the Cybersecurity Skills Gap Requires a Global Effort

This is a summary of an article written by Ken Xie, Fortinet's founder and CEO, that first appeared on the World Economic Forum Agenda blog on 23 Jan 2019. Read more about Fortinet's leadership with WEF's Centre for Cybersecurity.

Organizations worldwide are struggling to keep up with cybercrime. Even though Gartner predicts worldwide spending on Information Security will reach $124 billion this year, security researchers estimate that the cost of cybercrime will outpace that spend by over 16X, reaching $2.1 trillion by the end of 2019.

Of course, part of the challenge is that many cybersecurity tools and strategies are not up to the task of protecting today's evolving networks. Many security developer and manufacturers need to reassess their strategies to include creating solutions that can span different environments and be integrated together into a unified security fabric.

The larger problem, however, is that there are simply not enough skilled humans available to properly plan, manage, integrate, and optimize security devices, strategies, and protocols.

> *"According to a recent workforce development survey, 59% of organizations have unfilled cybersecurity positions, with Frost & Sullivan forecasting a shortfall of 1.5 million by 2020. There are two reasons for this. The first is that the expansion of the digital marketplace has generated more jobs than the current supply of security professionals can meet. The second is a problem of scale, there is currently not an efficient way to create skilled security practitioners at the same rate."*

World Economic Forum Agenda blog

This growing security challenge is reaching a critical point. Failure to address it now has the potential to disrupt the emerging global digital economy. Governments, organizations, and educational institutions need to work together to address this challenge. This as one of the most urgent tasks facing the newly formed WEF Centre for Cybersecurity.

Here are five critical approaches according to Fortinet's Founder ad CEO Ken Xie, which we can start moving on today:

1. Develop hands-on training and apprenticeship programs that span organizations and government agencies in order to cross-train security professionals.
2. Update our formal educational process to emphasize careers in cybersecurity, and encourage more diversity among women and minorities.
3. Sponsor technical labs for secondary education and university programs, provide mentors, fund scholarships, and create cybersecurity internships.
4. Leverage military veterans transitioning to civilian life that already have exposure to many of the latest IT and security tools.
5. Accelerate our adoption of automation and machine learning so we can detect and respond to new threats at digital speeds and focus limited security personnel on higher order tasks.

We need to start now

When any infrastructure or economic system is brought down, everyone suffers. But as businesses and governments, including critical infrastructures, become increasingly interconnected, a major security event could have catastrophic consequences.

> *"Institutions like the World Economic Forum need to mount a global response to the global threat of cybercrime. This includes committing intellectual and financial resources toward solving the growing problem of the cybersecurity skills gap. We cannot afford to wait."* World Economic Forum Agenda blog

For more details on this topic, refer to the entire article, "*Here's how we can tackle the growing cybersecurity skills gap*," posted to the World Economic Forum's cybersecurity website.

Explore *The CISO Collective* - an online content hub and mobile application that provides CISOs with one stop to find the most relevant news and information to enable them to be more effective in their roles.

Read more about how Fortinet is working to solve the cyber skills gap with our Network Security Expert program, Network Security Academy program or our FortiVets program.

Source: *https://www.fortinet.com/blog/business-and-technology/addressing-the-cybersecurity-skills-gap-requires-a-global-effort.html*

15. Social Engineering Training: Why Getting Hacked Is a Security Advantage

It was one of the highest phishing rates I had ever seen: Almost 60 percent of employees clicked the malicious link. Yet the client, a chief information security officer (CISO) of a Fortune 100 company, asked a question that caught me completely off-guard.

"So, what?" he said, clearly unimpressed.

As a "people hacker" for X-Force Red, IBM Security's team of veteran hackers, I've performed social engineering exercises for companies around the world. There seem to be a lot of misconceptions about my job and the usefulness of social engineering assessments in security audits.

Confronted with that CISO's indifference, I tried to explain exactly how serious our findings were and what the consequences might mean for the business.

During this assessment, my team started off by getting several payloads through the company's email filters undetected. We identified that only two of the 300 employees reported the phishing email. The incident response (IR) team didn't start its investigation until two days later; during those two days, we managed to infiltrate some of the legal team's email accounts, where we discovered that the company was the target of a lawsuit that wasn't yet public. If that lawsuit were to leak, it could significantly hurt the company's reputation.

Additionally, by reusing some of the passwords we had compromised, we were able to log in to multiple employee payroll accounts, where we had access to direct deposit information — again, undetected. A criminal attacker could have changed direct deposit account numbers to siphon funds from employee paychecks.

My answer seemed to surprise the CISO and his team. In the end, they acknowledged that I provided a lot more information about their security posture than they expected to receive from the assessment.

Learn more at the Jan. 29 webinar

Components of a Quality Social Engineering Assessment

If you ask someone to define a social engineering assessment, they would most likely say it tests the human aspect of security. However, if done correctly, it evaluates much more than that. Yes, assessments track how many times employees click a link, open an attachment or divulge sensitive information to a suspicious recipient on the phone. However, they can also assess if and how employees are reporting suspicious activity, and the effectiveness of IR and security awareness training programs.

With a well-designed assessment, the client should have a better understanding of how their IR team handles social engineering attacks. Many components of IR programs can be analyzed by answering questions such as:

- How much time did it take for the IR team to respond to the social engineering activity?
- Did the IR team follow any playbooks?
- Did the team determine which employees knowingly or unknowingly divulged credentials, and did they issue password resets for those users?
- If employees provided their credentials, did the IR team investigate whether those credentials were being used elsewhere as part of a suspicious activity?

In this type of engagement, we test more than just people and processes; we can assess the effectiveness of security technologies too. Many of the actions performed — such as emailing a malicious payload, having an employee open a malicious USB device on their workstation, etc. — attempt to bypass different types of technologies in places such as email filters, intrusion detection systems (IDSs), antivirus software and more. Social engineering attack vectors test deployed technology to determine whether the social engineer can bypass them.

Effectiveness and Ethics of Social Engineering

Some critics have argued that social engineering assessments are pointless, as they know employees will always fail against such an attack. But these assessments provide valuable metrics, which are important to track over time to identify how employees are performing and identify any major deviations. Often, individual employees fall victim repeatedly. It's important to identify these users so they can receive additional training, and the company should ensure those accounts have limited access.

Others have pointed to social engineering tests that went too far, such as targeting employees' personal accounts. Each social engineering consultancy tests differently. That's why it's important for security leaders to define what's acceptable for the company, so that testers don't cross any ethical lines. This conversation between security leaders and testers typically happens during the scoping process.

Here's another common refrain: "We already have a security awareness training program in place, and it covers social engineering." But how do you know the program is effective? Without properly testing it, there is no way to determine whether it could efficiently and successfully contain an attack. Plus, employees should have continuous opportunities to identify social engineering activities. It is not a one-and-done exercise. Social engineering exercises are the most realistic training employees can get outside of an actual attack.

How a Box of Doughnuts Can Breach Your Defenses

Some of the social engineering assessments performed by X-Force Red include physical tests, such as walking into a building carrying a box of doughnuts to get past security, and remote tests, such as impersonating an auditor to trick employees into divulging sensitive corporate data over the phone. For each test, only a limited amount of company insiders know we are coming, and we scope the project ahead of time to ensure it is effective and ethical.

I can't give away all our tricks of the trade, but you'll have an opportunity to hear from five X-Force Red hackers, including me, when we share our greatest hits and best practices during a one-hour webinar on Jan. 29 at 11:00 a.m. EST. You may be surprised by some of the many ruses that get us through the door.

Source: https://securityintelligence.com/social-engineering-training-why-getting-hacked-is-a-security-advantage

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

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 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'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 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.