



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

Monthly Security Bulletin

May 2019

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!

Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation					
Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			
				Lite Plan	Professional Plan (incl. all from Lite)	Advanced Plan (incl. all from Professional)

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.

Table of Contents:

Executive Summary	4
1. 540 Million Facebook User Records Leaked by Public Amazon S3 Buckets.....	6
2. Cybercrime Market with Roughly 385,000 Members Found on Facebook	8
3. Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days	10
4. Criminal Market Sells Over 60K Digital Identities For \$5-\$200.....	11
5. New TajMahal Cyberespionage Kit Includes 80 Malicious Modules.....	14
6. Yahoo Offers \$117.5M Settlement in Data Breach Lawsuit.....	16
7. TicTocTrack Smartwatch Flaws Can Be Abused to Track Kids.....	17
8. Malvertising Campaign Abused Chrome to Hijack 500 Million iOS User Sessions	19
9. Unsecured Databases Leak 60 Million Records of Scraped LinkedIn Data.....	21
10. Cybercrime's Total Earnings Skyrocketed to \$2.7 Billion Says the FBI.....	25
11. Over 500% Increase in Ransomware Attacks Against Businesses	28
12. Zero Trust: Why Your Most Privileged Users Could Be Your Biggest Security	
Weakness.....	30
13. Old Vulnerabilities Are Still Good Tricks for Today's Attacks	31

Executive Summary

1. More than 540 million records of Facebook users have been leaked on Amazon S3 publicly accessible buckets used by 2 third-party apps. Although Facebook is not at fault here, it has been rough year for the social media giant and it shows a pattern of vulnerability. To learn more [Jump to article](#).
2. "An online black market offering cybercrime goods and services was found on Facebook, spreading over 74 groups and totaling around 385,000 members, according to a report by Cisco Talos security researchers." To learn more [Jump to article](#).
3. "HOYA Corporation was hit by a cyber attack at the end of February which led to a partial shutdown of its production lines from Thailand for three days." According to a company official no customer data was leaked due to the company interference in a timely manner, however the Japanese optical products manufacturer suffered overall industrial output level of the manufacturing plant dropping by roughly 60%. To learn more [Jump to article](#).
4. Kaspersky researchers have found a a market where over 60 000 stolen digital profiles are offered for sale for as little as 5 USD. The price can go to up to 200 depending on the value of the stolen information. To learn more [Jump to article](#).
5. "TajMahal, a previously unknown cyberespionage platform featuring roughly 80 different malicious modules and active since at least 2013, was discovered by Kaspersky Lab's research team during late 2018." To learn more [Jump to article](#).
6. Yahoo offers to pay 117,5 million USD settlement for one of the biggest data breach lawsuits. The tech company first offered 50M UDS, but the U.S, District Court refused the offer arguing that it's not nearly enough to cover losses and attorney expenses. To learn more [Jump to article](#).
7. "A popular smartwatch that allows parents to track their children's whereabouts, TicTocTrack, has been discovered to be riddled with security issues that could allow hackers to track and call children." To learn more [Jump to article](#).
8. "Multiple massive malvertising attacks which targeted iOS users from the U.S. and multiple European Union countries for almost a week used a Chrome for iOS vulnerability to bypass the browser's built-in pop-up blocker." To learn more [Jump to article](#).
9. "Eight unsecured databases were found leaking approximately 60 million records of LinkedIn user information. While most of the information is publicly available, the databases contain the email addresses of the LinkedIn users." To learn more [Jump to article](#).
10. "FBI's Internet Crime Complaint Center (IC3) published its 2018 Internet Crime Report which shows that cybercrime was behind \$2,7 billion in total losses during 2018 as shown by 351,936 complaints received during the last year." The report outlines worrying trend of 161% increase during 2918 compared with 2017. To learn more [Jump to article](#).
11. "Cybercriminals have started focusing their efforts on businesses during Q1 2019, with consumer threat detections decreasing by roughly 24% year over year while businesses

have seen a 235% increase in the number of cyber attacks against their computing systems.” To learn more [Jump to article](#).

12. Organization are focusing their efforts to protect their infrastructure from security breaches, but what to do if the threats come from the customers? Malicious actors are focusing on customers with privileged accounts. To learn more [Jump to article](#).
13. “The value of a security vulnerability drops significantly the moment it gets patched but the bad guys will keep exploiting it for as long as they can find victims that are worth the effort.” To learn more [Jump to article](#).

1. 540 Mllion Facebook User Records Leaked by Public Amazon S3 Buckets

More than 540 million records of Facebook users were exposed by publicly accessible Amazon S3 buckets used by two third-party apps to store user data such as plain text app passwords, account names, user IDs, interests, relationship status, and more.

As discovered by the UpGuard Cyber Risk team, Mexico-based media company [Cultura Colectiva](#) stored the records of roughly 540 million of its users within a 146 GB database called "cc-datalake," stored in a misconfigured Amazon S3 bucket which gave anyone download permissions.

This huge collection of Facebook records contained "comments, likes, reactions, account names, FB IDs and more," allowing Cultura Colectiva to "to tune an algorithm for predicting which future content will generate the most traffic."

Filename	Size	Modified
cc-datalake	--	Unknown
avro	--	Unknown
data	--	Unknown
datamodel	--	Unknown
page_feed_avro	--	Unknown
pagefeed_avro	--	Unknown
pagefeed_avro_test	--	Unknown
parquet	--	Unknown
tmp	--	Unknown
avro	--	Unknown
pagefeed_2017	--	Unknown
rediff_test	--	Unknown
whfb.zip	18.3 GiB	3/30/2018 10:02:48 AM
webhooksBk.zip	93.0 MiB	6/11/2018 11:20:39 AM
webhooks09052018.zip	108.6 MiB	6/11/2018 11:20:57 AM
webhooks20180507.zip	197.3 MiB	6/11/2018 11:21:36 AM
webhooks20180521.zip	122.2 MiB	6/11/2018 11:21:58 AM
webhooks20180526.zip	221.0 MiB	6/11/2018 11:22:30 AM
webhooks.zip	72.0 MiB	6/11/2018 11:22:47 AM
webhooksBk.log	7.7 MiB	6/13/2018 7:47:15 AM
webhooks20180526.log	709.5 KiB	6/13/2018 7:47:28 AM
webhooks20180521.log	411.0 KiB	6/13/2018 7:47:36 AM
webhooks20180507.log	782.9 KiB	6/13/2018 7:47:43 AM
webhooks.log	211.2 KiB	6/13/2018 7:48:35 AM
webhooks09052018.log	420.9 KiB	6/13/2018 7:48:44 AM
webhooks_test.zip	988 B	6/27/2018 8:26:26 PM
cc-data-acq-fbwhjson.gz	897.5 MiB	11/6/2018 9:55:40 AM
cc-data-acq-fbwhgz	1001.1 ...	11/7/2018 1:34:55 PM
CC_DATA_MODEL_LZ_FACEBOOK_WEBHOOKS_V3_1_PAGE_FEED_PAGEFEED.avro	560.6 MiB	11/26/2018 10:59:41 AM

Cultura Colectiva dataset

```

{
  "id": "ObjectId("587537614fcee50cae0abb61")",
  "Field": "Feed",
  "value": {
    "parent_id": " ",
    "sender_name": " ",
    "comment_id": " ",
    "sender_id": " ",
    "item": "comment",
    "verb": "add",
    "created_time": "1484076891",
    "post_id": " ",
    "message": " "
  }
}

{
  "id": "ObjectId("587537614fcee50cae0abb62")",
  "Field": "Feed",
  "value": {
    "reaction_type": "love",
    "parent_id": " ",
    "sender_id": " ",
    "item": "reaction",
    "verb": "add",
    "created_time": "1484076892",
    "post_id": " "
  }
}

{
  "id": "ObjectId("587537614fcee50cae0abb63")",
  "Field": "Feed",
  "value": {
    "parent_id": " ",
    "sender_name": " ",
    "sender_id": " ",
    "item": "like",
    "verb": "add",
    "created_time": "1484076892",
    "post_id": " "
  }
}

```

Cultura Colectiva dataset redacted sample

Another database pertaining to the now-defunct third-party Facebook-integrated "At the Pool" app (an archived version of the website [HERE](#)) with **only** 22,000 was also found by UpGuard in a downloadable S3 bucket but, unfortunately, this one also contained app user passwords in plain text.

"The passwords are presumably for the "At the Pool" app rather than for the user's Facebook account, but would put users at risk who have reused the same password across accounts," says Upguard.

In addition, At the Pool's leaked database came with "fk_user_id, fb_user, fb_friends, fb_likes, fb_music, fb_movies, fb_books, fb_photos, fb_events, fb_groups, fb+checkins, fb_interests, and more" user data points.

While this database did not leak the huge amount of data contained in the exposed Cultura Colectiva database, the fact that it belongs to a company which ceased its operations five years ago in 2014 makes one think of how many other similar AWS instances are left out there ready to be downloaded and used in credential stuffing or similar types of malicious attacks.

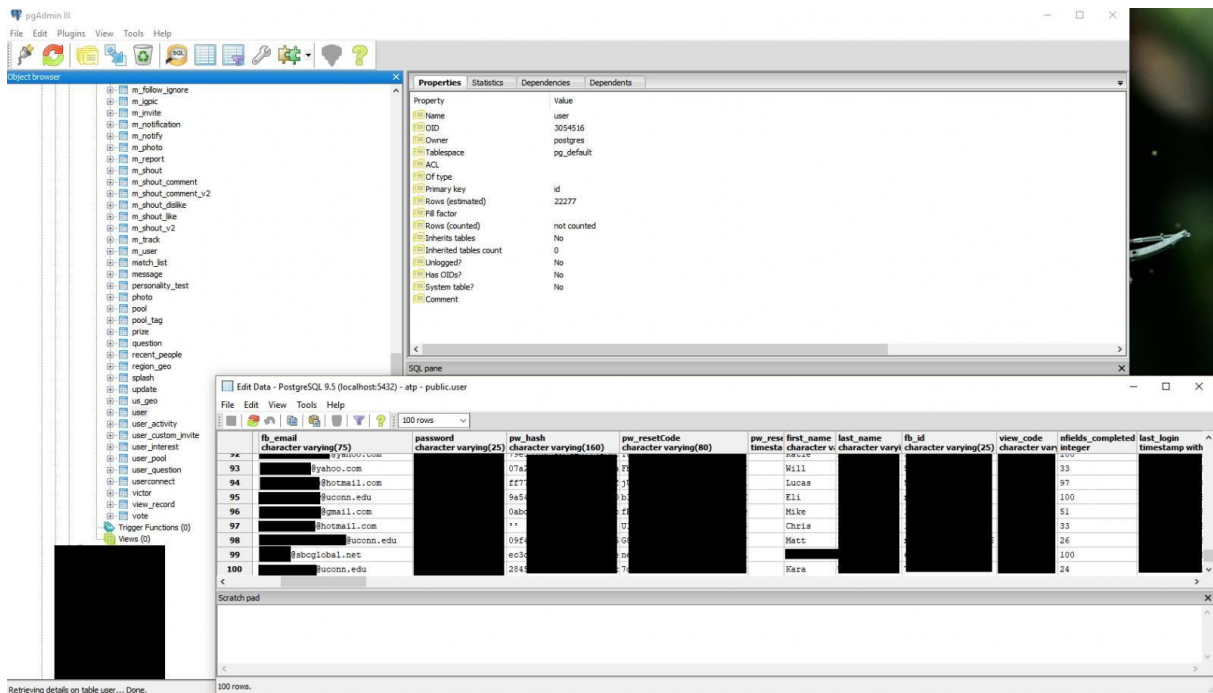


Figure 1. At the Pool dataset redacted sample

There are other similarities when taking into account the two Facebook user data sets leaked by misconfigured Amazon S3 buckets beside the number of users who got their sensitive personal info exposed, like the fact that they are both describing the users' "interests, relationships, and interactions, that were available to third-party developers."

While Facebook is now trying to cover their angles saying that user privacy is one of their main goals, user data collected by third-party apps is already out there, stored in the cloud within databases that might or might not be protected adequately.

[Upguard says](#) that they contacted Cultura Colectiva to let them know they're leaking their users' data on both January 10 and January 14 but they did not receive an answer. However, after getting in touch with Amazon Web Services on January 28, they were informed that the company was in the end made aware of the data leak on February 1.

After another exchange and an intervention from Bloomberg who asked for comment on the issue, the cc-datalake database was eventually secured on April 3.

The At the Pool database, in turn, was removed during UpGuard's investigation to confirm its owner and, at the moment, the user data which it got leaked is no longer available for anyone to access.

Not the first time it happens

While Facebook is not behind the two leaked databases, the company certainly went through a rough year or so, seeing that it [disclosed a security vulnerability](#) which impacted around 50 million people in September 2018, a security flaw that potentially enabled malicious actors to access sensitive info of all affected users.

During December, [a bug in the platform's Photo API](#) may have also allowed attackers to gain unauthorized access to protected photos of roughly 6.8 million Facebook users.

Also, in November, an underground forum seller going by the name "FBSaler" auctioned [the information of 120 million Facebook users](#) as well as the private messages of another 81,000 profiles for 10 cents each.

Source: <https://www.bleepingcomputer.com/news/security/540-million-facebook-records-leaked-by-public-amazon-s3-buckets/>

2. Cybercrime Market with Roughly 385,000 Members Found on Facebook

An online black market offering cybercrime goods and services was found on Facebook, spreading over 74 groups and totaling around 385,000 members, according to a report by Cisco Talos security researchers.

"The majority of these groups use fairly obvious group names, including 'Spam Professional,' 'Spammer & Hacker Professional,' 'Buy Cvv On THIS SHOP PAYMENT BY BTC,' and 'Facebook hack (Phishing),' says Cisco Talos.

More to the point, the members of these Facebook groups sell, buy, and exchange anything from account credentials and phishing tools and services credit card info and fake IDs.

"Others products and services were also promoted. We saw spammers offering access to large email lists, criminals offering assistance moving large amounts of cash, and sales of shell accounts at various organizations, including government," also said the Cisco Talos researchers.

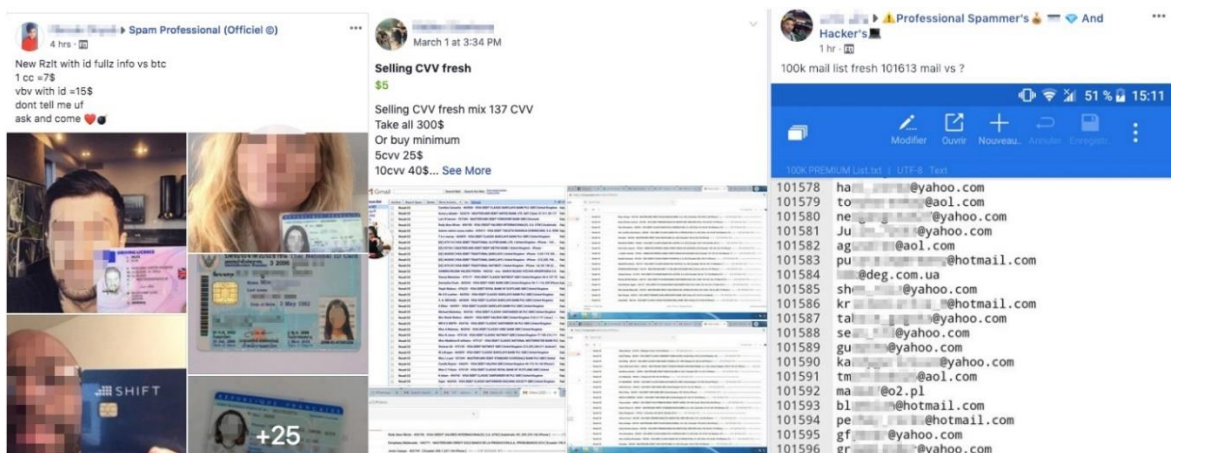


Figure 2. Sample Facebook posts offering illegal services and goods

What's even more surprising is that it is very simple to find and join these cybercrime-focused Facebook groups, especially since Facebook's algorithms will automatically suggest joining similar groups from the same network designed to promote illegal cybercrime tools and services.

While Cisco Talos first tried to take down the groups using the social network's [abuse report feature](#), the security researchers had to eventually reach out to Facebook and disclosed their findings after their initial attempts weren't fully successful.

This led to the eventual takedown of most of the Facebook groups involved in the virtual black market, but, as [reported by Cisco Talos](#), new groups have been created and some of them are still active and need to be closed by the social network's security team.

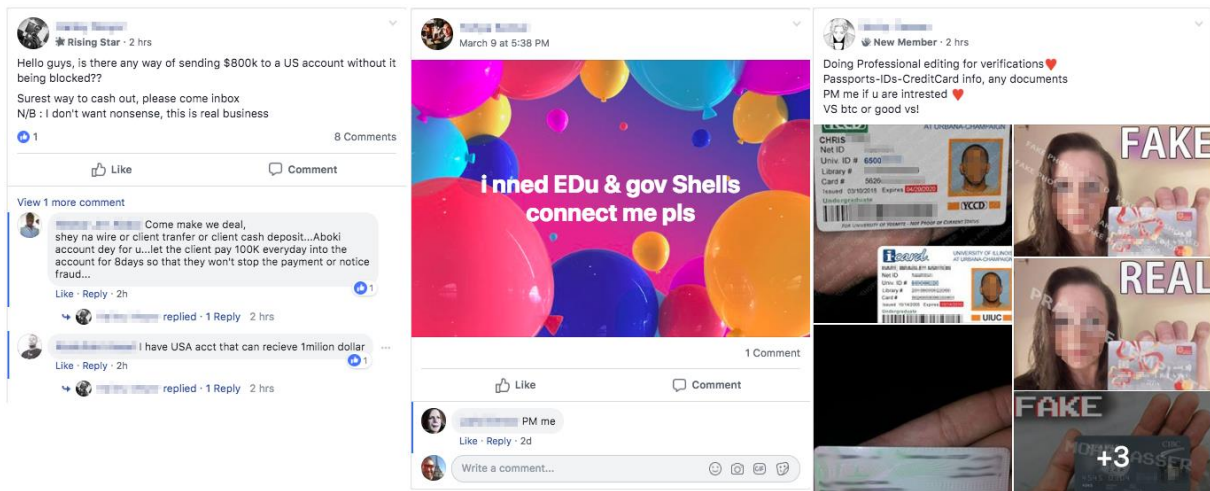


Figure 3. More sample Facebook posts offering illegal services and goods

This is definitely not the first time this type of activity has been found on Facebook, with [Brian Krebs](#) previously reporting about 120 private Facebook groups with over 300,000 members who exchanged illicit services and tools.

According to Krebs, who also provided a [spreadsheet](#) with the full list of groups found to engage in this type of activities, "The scam groups facilitated a broad spectrum of shady activities, including spamming, wire fraud, account takeovers, phony tax refunds, 419 scams, denial-of-service attack-for-hire services and botnet creation tools."

The big issue behind the reoccurrence of these groups is Facebook's reliance on their members' willingness to report themselves.

And, as Cisco Talos concludes, "As a consequence of this, a substantial number of cyber-scammers have continued to proliferate and profit from illegal activities. Operating with impunity, these attackers relentlessly probe cyber-defenses of enterprises everywhere."

Source: <https://www.bleepingcomputer.com/news/security/cybercrime-market-with-roughly-385-000-members-found-on-facebook/>

3. Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days

Japanese optical products manufacturer HOYA Corporation was hit by a cyber attack at the end of February which led to a partial shutdown of its production lines from Thailand for three days.

The company disclosed that around 100 computers were infected with a malware strain designed to steal user credentials from the machines it compromises and to drop a cryptocurrency miner during the infection process' second stage.

As reported by multiple local sources ([The Japan Times](#), [Kyodo News](#), [SankeiBiz](#)), HOYA Corp. was able to block the attackers' cryptojacking attempt after the credential-stealing malware put an abnormal load on a network server which led to the quick discovery of the attack.

Following the initial phase of the attack, the workers were no longer able to effectively take care of orders with the overall industrial output level of the manufacturing plant dropping by roughly 60%.

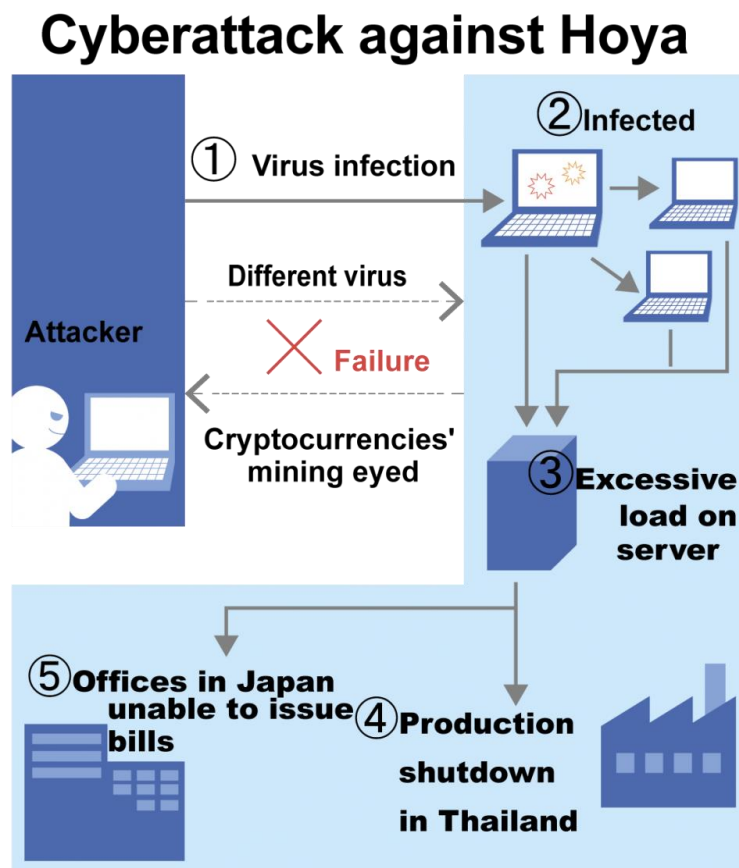


Figure 4. (Image: KYODO NEWS)

The IT computing system of the Thailand plant was not the only victim given that the computers at the Japanese headquarters were also impacted, making it harder to issue invoices during the incident.

While the cyber attack had limited impact on HOYA's business and no data was leaked according to a company official, the production delay caused by the incident is still affecting the manufacturer seeing that its plants have no downtime.

Toyota and Norsk Hydro also under attack this year

HOYA Corp. is not the only company affected by cyber attacks lately, with multiple [Toyota and Lexus sales subsidiaries being breached](#) at the end of March, leading to the personal information of roughly 3.1 million Toyota customers possibly being leaked.

In addition, also during March, the Norsk Hydro aluminum company was [forced to switch to partial manual operations](#) after a cyber attack that pushed LockerGoga ransomware impacted its production plants.

In January, LockerGoga was also used to attack the network of engineering consulting firm [Altran Technologies](#), which was subsequently forced to shut down its entire IT network to protect the company's data.

Source: <https://www.bleepingcomputer.com/news/security/cyber-attack-shuts-down-hoya-corps-thailand-plant-for-three-days/>

4. Criminal Market Sells Over 60K Digital Identities For \$5-\$200

More than 60,000 stolen digital profiles are currently up for sale on Genesis Store, a private and invitation-only online cybercriminal market discovered and exposed by Kaspersky Lab researchers.

"The profiles include: browser fingerprints, website user logins and passwords, cookies, credit card information. The price varies from 5 to 200 dollars per profile – it heavily depends on the value of the stolen information," said the researchers.

A digital fingerprint is a complex collection of system properties—up to 100 attributes, from IP addresses, screen size, device ID, timezone, GPU/CPU info, cookies, and many others—and user behavioral characteristics that can range from the user interests and custom system configuration changes to the time spent on specific websites and mouse movement behavior.

The digital profiles available for sale on the Genesis Store cybercriminal marketplace were stolen from users who got infected by malware strains designed for this specific purpose: to collect and exfiltrate accounts, logins, passwords, and browsers cookies and send them to their masters.

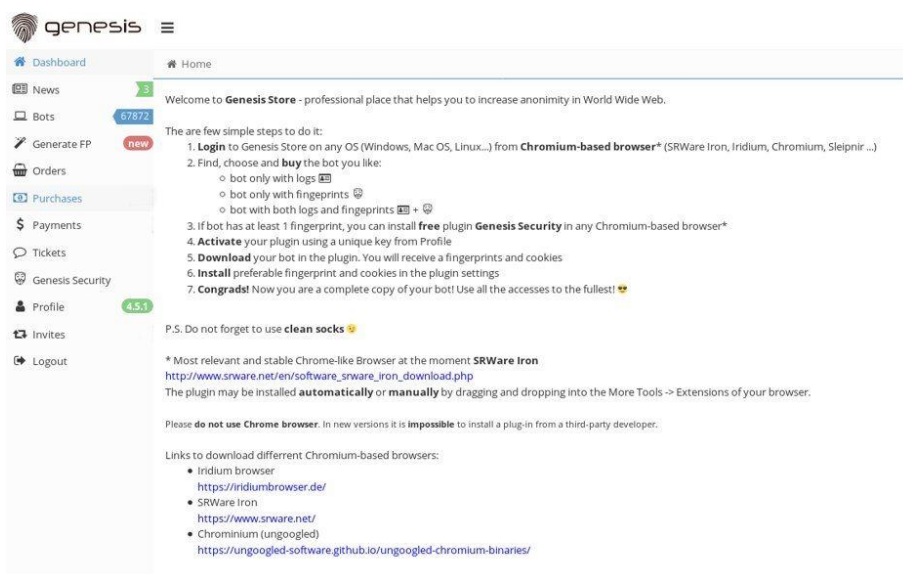


Figure 5. Genesis Store home page

What makes digital identities a marketable commodity on cybercriminal markets is the fact that they are used to circumvent fraud detection systems put in place by online stores, banks, and various other services which are a common target for malicious actors.

While cybercriminals are able to steal both user credentials and payment card info and, in theory, put them to work by logging into their victims' online banking systems, the bank's anti-fraud system will block such attempts by comparing their digital fingerprint against a database of digital identities of known miscreants.

Besides the digital fingerprints sold to crooks who need them to replace their systems' fingerprints with fake ones, the threat actors behind Genesis Store also sell a wide assortment of stolen data "including user accounts, logins, passwords and browser cookies collected from various online services – from stores and payment systems to bank accounts."

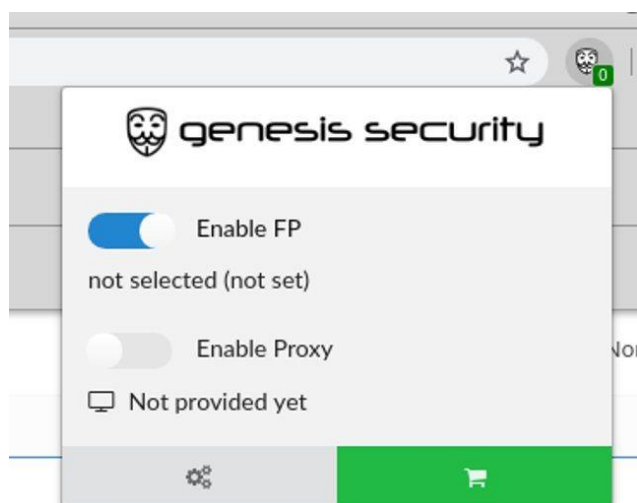
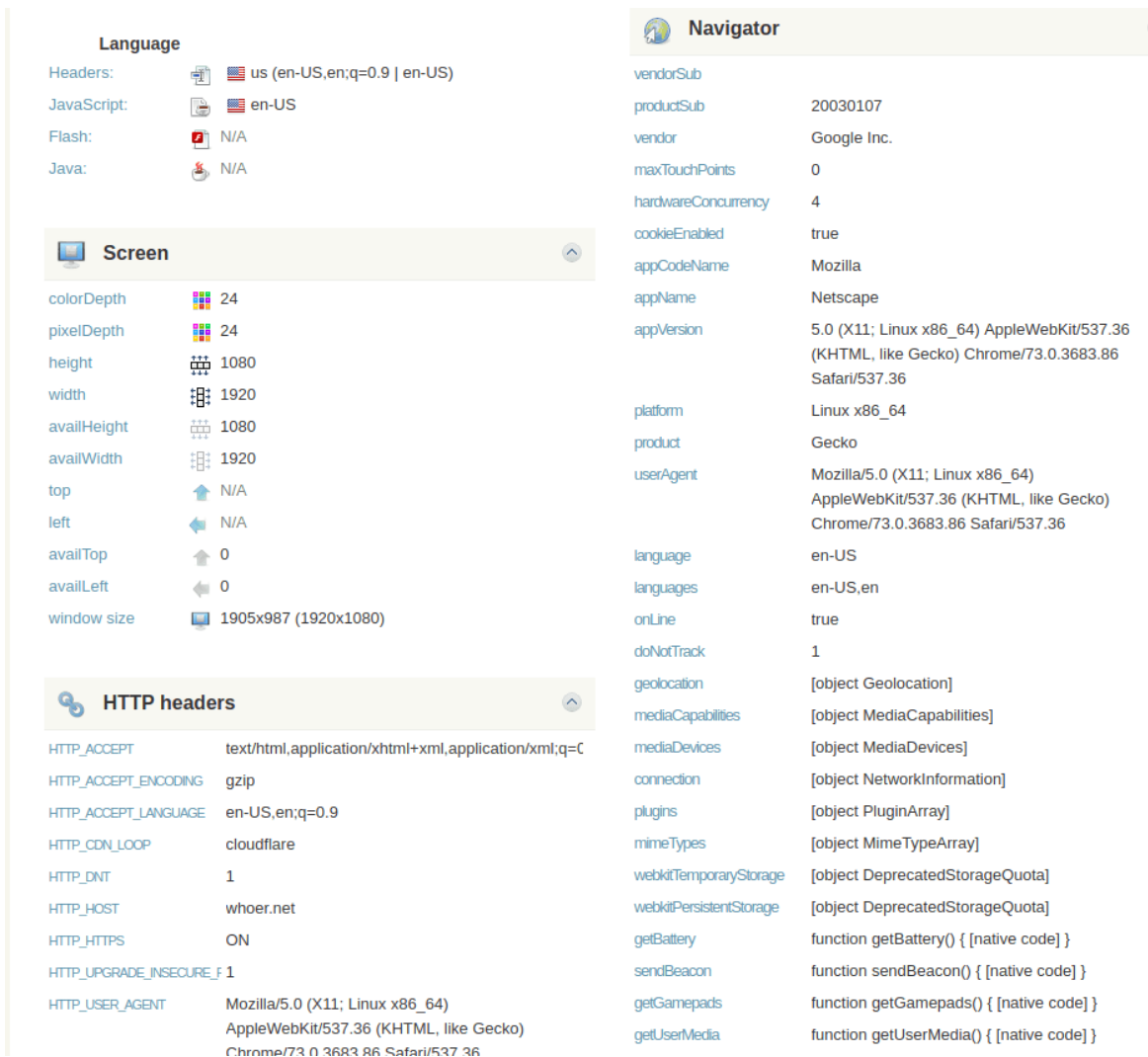





Figure 6. Digital doppelganger Chromium extension




Language

Headers:  us (en-US,en;q=0.9 | en-US)

JavaScript:  en-US

Flash:  N/A

Java:  N/A

Screen

colorDepth: 24

pixelDepth: 24

height: 1080

width: 1920

availHeight: 1080

availWidth: 1920

top: N/A

left: N/A

availTop: 0

availLeft: 0

window size: 1905x987 (1920x1080)

HTTP headers

HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9

HTTP_ACCEPT_ENCODING: gzip

HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.9

HTTP_CDN_LOOP: cloudflare

HTTP_DNT: 1

HTTP_HOST: whoer.net

HTTP_HTTPS: ON

HTTP_UPGRADE_INSECURE_F: 1

HTTP_USER_AGENT: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36

Navigator

vendorSub:

productSub: 20030107

vendor: Google Inc.

maxTouchPoints: 0

hardwareConcurrency: 4

cookieEnabled: true

appName: Mozilla

appName: Netscape

appVersion: 5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36

platform: Linux x86_64

product: Gecko

userAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36

language: en-US

languages: en-US,en

onLine: true

doNotTrack: 1

geolocation: [object Geolocation]

mediaCapabilities: [object MediaCapabilities]

mediaDevices: [object MediaDevices]

connection: [object NetworkInformation]

plugins: [object PluginArray]

mimeType: [object MimeTypeArray]

webkitTemporaryStorage: [object DeprecatedStorageQuota]

webkitPersistentStorage: [object DeprecatedStorageQuota]

getBattery: function getBattery() { [native code] }

sendBeacon: function sendBeacon() { [native code] }

getGamepads: function getGamepads() { [native code] }

getUserMedia: function getUserMedia() { [native code] }

Figure 7. Digital fingerprint example

The Genesis Store market comes with a built-in search panel which allows buyers to quickly find a specific profile using a wide assortment of filters and, even more importantly, a .crx plugin for Chromium-based web browsers to make it as easy as possible to quickly add the stolen digital profiles to one's browser with a single mouse click.

Once a digital profile has been applied to the cybercriminal's browser, the bad actor will become a virtual doppelganger of the user who got his digital fingerprint stolen—and potentially his logins and passwords, cookies, credit card information—the only thing left to do for the crook being to connect to the website it wants to target using a VPN or proxy also appear to be located near the victim's real location.

The Genesis Store operators also provide cybercriminals with the choice to generate random and unique fingerprints that can be used to login within online services that employ digital identity-based anti-fraud without triggering any sort of alarms.

As detailed in a Juniper Research [study from 2018](#), "annual online payment fraud losses from eCommerce, airline ticketing, money transfer and banking services, will reach \$48 billion by 2023; up from the \$22 billion in losses projected for 2018."

This makes fighting identity theft and fraud schemes a top concern for all companies in the financial industry which, as advised by Kaspersky Lab's research team can protect their users against attackers using digital profiles to impersonate their victims by enabling two-factor authentication for any and all transactions made online.

"Even though it is not very convenient for users to complete the extra authentication routine each time they want to buy online, it is the most effective safeguard against carding attacks for the present," [concluded Kaspersky Lab](#).

Source: <https://www.bleepingcomputer.com/news/security/criminal-market-sells-over-60k-digital-identities-for-5-200/>

5. New TajMahal Cyberespionage Kit Includes 80 Malicious Modules

TajMahal, a previously unknown cyberespionage platform featuring roughly 80 different malicious modules and active since at least 2013, was discovered by Kaspersky Lab's research team during late 2018.

Even though it was active for the past six years, "with the earliest sample dated April 2013, and the most recent August 2018," the advanced persistent threat (APT) framework is not yet connected to any hacking groups.

As further found by Kaspersky Lab, TajMahal is a multi-stage attack framework which comes with two malicious packages, self-named as Tokyo and Yokohama, dropped one after the other on the target's computer.

The smaller Tokyo package deployed during the first infection stage comes with backdoor functionality and is used to drop the fully-featured Yokohama spying package which features around "80 modules in all, and they include loaders, orchestrators, command and control communicators, audio recorders, keyloggers, screen and webcam grabbers, documents and cryptography key stealers."

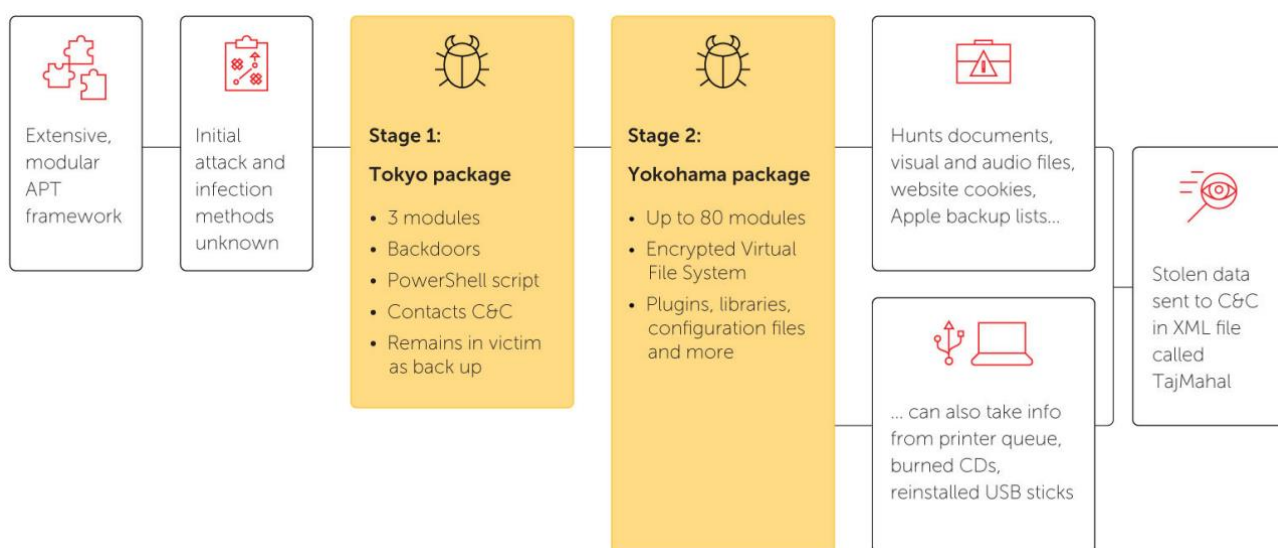


Figure 8. The TajMahal APT framework

All the systems where the researchers found the TajMahal framework in the wild were infected by both Tokyo and Yokohama, which hints at both of them remaining functional on the compromised machines, inferring "that Tokyo was used as first stage infection, deploying the fully-functional Yokohama package on interesting victims, and then left in for backup purposes."

Once Yokohama gets dropped on a victim's computer, it is used to hunt down interesting documents and media files, steal cookies and backups, swipe files from the printer queue, burned CDs, and from USB storage devices.

All this collected data is subsequently sent to a command-and-control server controlled by the hacking group behind the APT framework in the form of an XML file named TajMahal.

Because a central Asian diplomatic entity is the only confirmed TajMahal victim by the researchers, with the attack taking place back in 2014, despite the framework being used for at least five years, Kaspersky Lab' theorized that there are other targets which had their computing systems compromised using this cyberespionage platform.

Some of the capabilities discovered by Kaspersky Lab's researchers while examining the [TajMahal framework](#):

- Capable of stealing documents sent to the printer queue.
- Data gathered for victim recon includes the backup list for Apple mobile devices.
- Takes screenshots when recording VoicelP app audio.
- Steals written CD images.
- Capable of stealing files previously seen on removable drives once they are available again.
- Steals Internet Explorer, Netscape Navigator, FireFox and RealNetworks cookies.

- If deleted from Frontend file or related registry values, it will reappear after reboot with a new name and startup type.

Kaspersky Lab lead malware analyst [Alexey Shulmin said](#), "The TajMahal framework is a very interesting and intriguing finding. The technical sophistication is beyond doubt and it features functionality we have not seen before in advanced threat actors. A number of questions remain. For example, it seems highly unlikely that such a huge investment would be undertaken for only one victim."

Also, "This suggests that there are either further victims not yet identified, or additional versions of this malware in the wild, or possibly both. The distribution and infection vectors for the threat also remain unknown. Somehow, it has stayed under the radar for over five years. Whether this is due to relative inactivity or something else is another intriguing question. There are no attribution clues nor any links we can find to known threat groups."

Source: <https://www.bleepingcomputer.com/news/security/new-tajmahal-cyberespionage-kit-includes-80-malicious-modules/>

6. Yahoo Offers \$117.5M Settlement in Data Breach Lawsuit

Yahoo is offering to cough up \$117.5 million to settle a lawsuit regarding its massive data breaches that compromised the personal information of three billion users.

The [new \\$117.5 million settlement](#), filed Tuesday in the U.S. District Court in San Jose, comes after the internet company's first settlement proposal of \$50 million was rejected in January. The lawsuit comes on the heels of massive breaches of Yahoo's systems between 2013 and 2016.

That includes Yahoo's infamous [2013 breach](#) that is believed to be one of the biggest in history, which resulted in 3 billion accounts becoming compromised. Stolen data included names, email addresses, hashed passwords and more.

In late 2014, the company fell victim to a [second breach](#) that compromised 500 million accounts; while it disclosed yet [another breach](#) in 2016, confirming that "an unauthorized third party accessed the company's proprietary code to learn how to forge cookies."

In 2017, Yahoo, which is now part of Verizon Communications, was [slapped with a class action lawsuit](#) alleging that the company did not disclose the data breaches fast enough.

In [January 2019](#), a first settlement proposal made by Yahoo was knocked down by U.S. District Court Judge Lucy Koh. The company proposed to pay \$50 million and offer two years

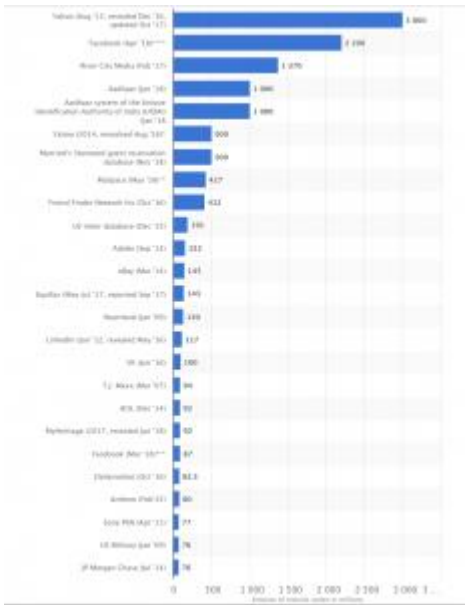


Figure 9. Credit: Statista

of free credit monitoring for 200 million people in the U.S. and Israel. However, [Koh said](#) that that settlement wasn't sufficient as it didn't specify how much money victims could expect to recover and didn't cover attorneys' fees.

This most recent settlement aims to assuage those concerns by having company paying for two years of free credit monitoring and "alternative compensation" for impacted victims; out-of-pocket expenses related to identifying theft, lost time, paid user costs, small business user costs; attorneys' fees and more. Koh has yet to make a decision regarding Yahoo's Tuesday settlement.

In April 2018, Yahoo also agreed to pay a [\\$35 million settlement](#) with the Securities and Exchange

Commission (SEC), which alleged that the company "misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts."

Source: <https://threatpost.com/yahoo-offers-117-5m-settlement-in-data-breach-lawsuit/143671/>

7. TicTocTrack Smartwatch Flaws Can Be Abused to Track Kids

A popular smartwatch that allows parents to track their children's whereabouts, TicTocTrack, has been discovered to be riddled with security issues that could allow hackers to track and call children.

Researchers at Pen Test Partners revealed vulnerabilities in the watch (sold in Australia) on Monday, which could enable hackers to track children's location, spoof the child's location or view personal data on the victims' accounts. The parent company of the TicTocTrack watch, iStaySafe Pty Ltd., has temporarily restricted access to the watch's service and app while it investigates further.

Researchers found that the service's back end does not make any authorization attempt on any request – besides the user having a valid username and password combination. That means that an attacker who is logged into the service could remotely compromise the app and track other accounts that are based in Australia.

"All in all we can see that the developer of the back end took no consideration into authorizing any of the requests, and cared only that the application was working effectively, leaving all the data available to access and manipulate," Pen Test Partners researcher Vangelis Stykas said in a [analysis](#). "This is unacceptable for a product that is supposed to keep children

secure and a trend that we constantly see in the IoT market that products are rushed to the market.”

The [TicTocTrack smartwatch](#) is made by Gator Group (which has had [watch privacy issues before](#)). The smartwatch also comes with a complementary mobile app, developed by a company called Nibaya, that is available on Google Play and the Apple App Store.



Figure 10. Tracking smartwatch coordinates

“To this day, there has never been a security breach that has led to our customer’s personal data being used for malicious purposes,” said iStaySafe in a statement sent to Threatpost. “Our team are constantly working to improve our software and make it as safe as possible for our users. As soon as a full technical assessment has taken place, conducted by a trusted, reputable and accredited penetration testing service, we will be releasing a transparent report which will detail what security issues were apparent, what steps we are taking and when.”

The smartwatch, available in Australia for \$149 (USD), is designed for children and uses GPS to track the movement of the wearer every six minutes, and offers voice calling and SMS features.

The smartwatch’s API can be attacked by changing the FamilyIdentifier number (which identifies the family that the user belongs to), which then could give a bad actor complete access to the user’s data – including the children’s location, parent’s full names, phone numbers and other personal identifiable information.

“Anyone could discover the location of children using the watch,” Stykas said. “Anyone could tamper with that position data, making you think your children were safe whilst they were actually elsewhere. Anyone could cause false alarms by moving the reported position of your child.”

Researchers with Pen Test Partners teamed up with security researcher Troy Hunt, who lives in Australia, to [test the attack](#). With Hunt’s daughter wearing the device, Pen Test Partners researchers found that they were able to successfully both track and spoof her location– as well as contact her via a phone call, which purported to be from “dad” on the watch.

In this video below, Hunt shows how the smartwatch vulnerability could be exploited to call his daughter – and how her smartwatch would answer automatically without any interaction needed from her end:

<https://www.youtube.com/watch?v=aAux7qW1Elw>

The company said in its notice to customers that they will restrict all use access to the TicTocTrack application and service until they can confirm the validity of the flaws and fix them.

Smartwatches continue to be a cause for security concern – particularly ones targeted at tracking children. In January, researchers found an array of [security issues](#) in the Gator portfolio

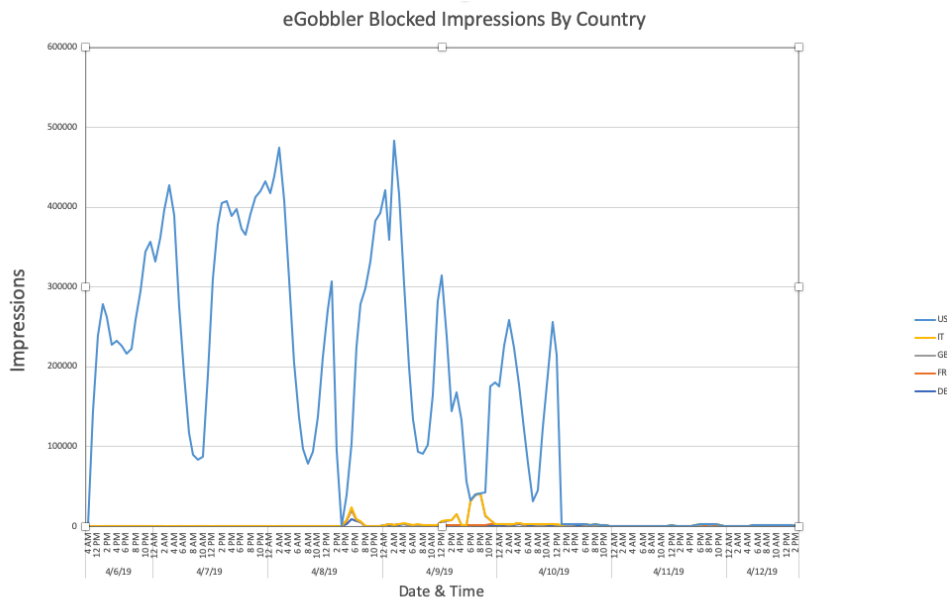


Figure 11. Graph of eGobbler Blocked Impressions By Country.

of watches from TechSixtyFour, and found flaws exposing sensitive data of 35,000 children. In [February](#), the European Commission issued a recall for the Safe-KID-One, an IoT watch made by German company Enox Group, due to “serious” privacy issues. And, in November, The Misafes “Kids Watcher” GPS watch [was found to have vulnerabilities](#) that translate into a stalker or pedophile’s ideal toolset.

Source: <https://threatpost.com/tictotrack-smartwatch-flaws-track-kids/143791/>

8. Malvertising Campaign Abused Chrome to Hijack 500 Million iOS User Sessions

Multiple massive malvertising attacks which targeted iOS users from the U.S. and multiple European Union countries for almost a week used a Chrome for iOS vulnerability to bypass the browser's built-in pop-up blocker.

eGobbler, the threat group behind the flurry of attacks, used "8 individual campaigns and over 30 fake creatives" throughout their push, with each of the fake ad campaigns having lifespans of between 24 and 48 hours.

In total, according to the Confiant researchers who discovered and monitored eGobbler's iOS-targeted attacks, roughly 500 million users sessions were exposed to this large scale orchestrated campaign pushing fake ads.

eGobbler's campaigns usually stay active for a maximum of 48 hours, immediately followed by short periods of hibernation which abruptly end when the next attack starts as discovered by Confiant's experts.

The April campaign used landing pages hosted on .world domains and it made use of pop-ups to hijack users sessions and redirect the victims to malicious landing pages.

While using pop-ups has been observed before as part of similar campaigns as the method used to redirect targets to pages designed by the malicious actors for phishing or malware dropping purposes, it's definitely an unusual one considering the effectiveness of browser pop-up blockers.

The crooks' decision to use pop-ups to hijack users sessions was revealed after the researchers tested the malvertising campaign's payloads "across over two dozen devices, both physical and virtual" and "split test this experiment between sandboxed and non-sandboxed iframes."

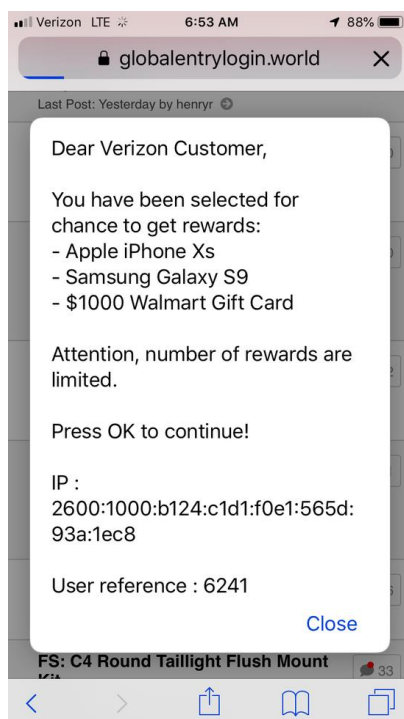


Figure 12. Malvertising campaign landing page

As they discovered, "the payload's main session hijacking mechanism was pop-up based, and furthermore, Chrome on iOS was an outlier in that the built-in pop-up blocker failed consistently."

The reason that happened was revealed to be the payload's inbuilt "techniques that took advantage of iOS Chrome's detection around user activated pop-up detection, resulting in the circumvention of pop-up blocking."

eGobbler Chrome for iOS exploit bypasses ad sandboxing attributes

To do that the malicious payloads used by the eGobbler group during these massive malvertising campaigns exploited a yet unpatched vulnerability in the Chrome for iOS web browser — the Chrome team is investigating the issue after Confiant reported the flaw on April 11.

To make things even worse, as Confiant further found, "the malvertising exploit leveraged by eGobbler is that it's not preventable by standard ad sandboxing attributes."

This means that the ad sandboxing attributes built within ad serving products such as Google's AdX and EBDA will also be circumvented by the payloads, as well as their user interaction requirement.

The fact that this exploit is able to bypass that need for user interaction should be impossible according to the same-origin policy as it pertains to cross-origin iframes. Furthermore, this completely circumvents the browser's anti-redirect functionality, as the attacker no longer needs to even spawn a redirect in order to hijack the user session.

This campaign was designed by the eGobbler malvertising group to specifically target iOS users but it was not the first. During [November 2018](#), Confiant monitored another campaign run by the ScamClub group which managed to hijack roughly 300 million iOS user sessions and redirected them all to adult content and gift card scams.

However, as [Confiant said in their report](#), "This really was a standout campaign compared to the others that we track based not only on the unique payload, but the volumes as well."

Also, "After a brief pause, the campaign saw a strategic pivot on April 14 to another platform and is currently still active under '.site' TLD landing pages. With half a billion user sessions impacted, this is among the top three massive malvertising campaigns that we have seen in the last 18 months."

Source: <https://www.bleepingcomputer.com/news/security/malvertising-campaign-abused-chrome-to-hijack-500-million-ios-user-sessions/>

9. Unsecured Databases Leak 60 Million Records of Scraped LinkedIn Data

Eight unsecured databases were found leaking approximately 60 million records of LinkedIn user information. While most of the information is publicly available, the databases contain the email addresses of the LinkedIn users.

Approximately two weeks ago, I was contacted by security researcher [Sanyam Jain](#) of the GDI foundation about something strange that he was seeing. Jain told BleepingComputer that he kept seeing unsecured databases containing the same LinkedIn data appearing and disappearing from the Internet under different IP addresses.

"According to my analysis the data has been removed every day and loaded on another IP. After some time the database becomes either inaccessible or I can no longer connect to the particular IP, which makes me think it was secured. It is very strange."

Between all eight databases, there was a combined total of approximately 60 million records that contained what appeared to be scraped public information of LinkedIn users. The total size of all of the 8 DBs is 229 GB, with each database ranging between 25 GB to 32 GB.



Figure 13. Example Database

As a test, Jain pulled my record from one of the databases and sent it to me for review. The data contained in this record included my LinkedIn profile information, including IDs, profile URLs, work history, education history, location, listed skills, other social profiles, and the last time the profile was updated.

Included in the profile was also my email address that I used when registering my LinkedIn account. It is not known how they gained access to this information as I have always had the LinkedIn privacy setting configured to not publicly display my email address.

```
"_id": "5b9b1174385f0a0036ac78fb",
  "email": " [REDACTED]@bleepingcomputer.com",
  "emails": [
    {
      "address": " [REDACTED]@bleepingcomputer.com",
      "type": null,
      "sha256": " [REDACTED] fb79ad616cb6320a",
      "domain": "bleepingcomputer.com",
      "local": " [REDACTED] "
    }
  ],
  "profiles": [
    {
      "network": "linkedin",
      "ids": [
        "37674468"
      ],
      "clean": "linkedin.com/in/lawrence-abrams-43074a1",
      "aliases": [
        "linkedin.com/pub/lawrence-abrams/10/74a/430"
      ],
      "username": "lawrence-abrams-43074a1",
      "url": "http://www.linkedin.com/in/lawrence-abrams-43074a1"
    }
  ],
```

Figure 14. Profile information for my record

After reviewing the data that was sent to me, I found all of the information to be accurate.

In addition to the above public information, each profile also contains what appears to be internal values that describe the type of LinkedIn subscription the user has and whether they utilize a particular email provider. These values are labeled "isProfessional", "isPersonal", "isGmail", "isHotmail", and "isOutlook".

```
"isProfessional": false,
"isPersonal": false,
"hasOtherNetwork": true,
"isGmail": false,
"isHotmail": false,
"isOutlook": false,
"linkedinUsername": "lawrence-abrams-43074a10",
"linkedin_profile": "http://www.linkedin.com/in/lawrence-abrams-43074a10",
"first_name": "Lawrence",
"last_name": "Abrams",
"country": "united states",
"state": "new york",
"city": "new york",
"industry": "Online Media",
"full_profile": {
  "companies": [
    {
      "current": false,
      "company_name": "Bleeping Computer",
      "company_position": "owner",
      "start_date": null,
      "end_date": null
    }
  ],
}
```

Figure 15. Internal Values

While we not able to determine who the database belonged to, we were able to contact Amazon who is hosting the databases for assistance in getting them secured. As of Monday, the databases were secured and are no longer accessible via the Internet.

LinkedIn states it's not their database

After seeing that the database contained a user's email addresses and what appeared to be possible internal values, BleepingComputer contacted LinkedIn to see if the database belonged to them.

After they reviewed my sample record, Paul Rockwell, head of Trust & Safety at LinkedIn, told us that this database does not belong to them, but they are aware of third-party databases containing scraped LinkedIn data.

"We are aware of claims of a scraped LinkedIn database. Our investigation indicates that a third-party company exposed a set of data aggregated from LinkedIn public profiles as well as other, non-LinkedIn sources. We have no indication that LinkedIn has been breached."

When we followed up with questions as to why the databases would contain my email, we were told that in some cases an email address could be public and were provided a [link to a privacy page](#) that allows you to configure who can see a profile's email address.

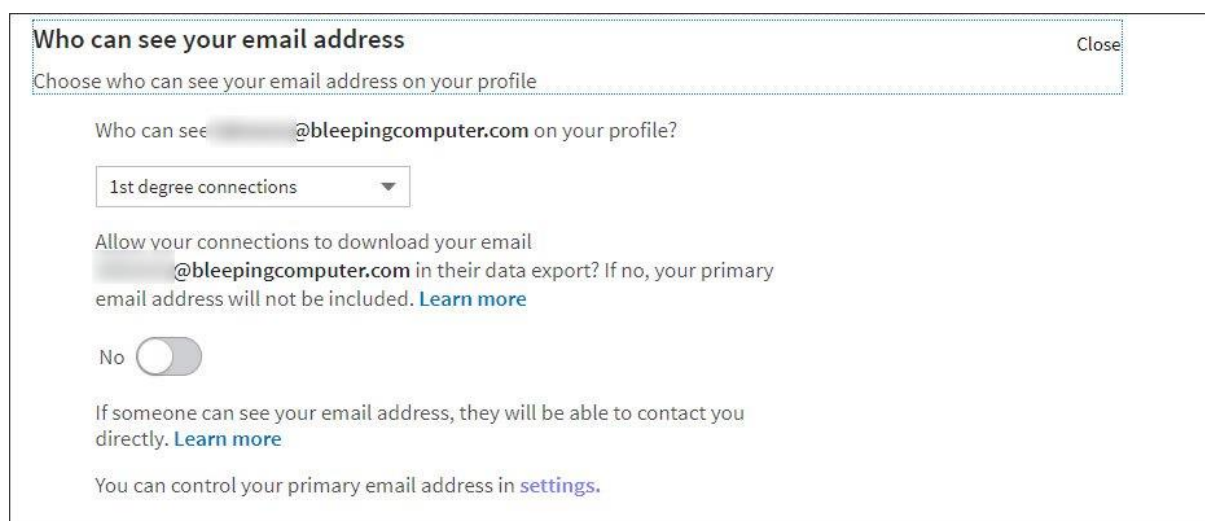


Figure 16. LinkedIn Email Privacy Settings

My settings only allow 1st degree connections to see my email address, so unless the scraper is posing as this type of connection, it is still not known how my email address was included in the database.

Source: <https://www.bleepingcomputer.com/news/security/unsecured-databases-leak-60-million-records-of-scraped-linkedin-data/>

10. Cybercrime's Total Earnings Skyrocketed to \$2.7 Billion Says the FBI

FBI's Internet Crime Complaint Center (IC3) published its 2018 Internet Crime Report which shows that cybercrime was behind \$2,7 billion in total losses during 2018 as shown by 351,936 complaints received during the last year.

Since its inception in May 2000, IC3 says that it has received 4,415,870 complaints, with an average of around 300,000 complaints each year and roughly 900 per day. These resulted in a total loss of \$7.45 billion over the last five years, between 2014 and 2018.

As further reported by the IC3, the internet crimes with the highest reported losses by their victims were BEC, confidence/romance fraud, and non-payment/non-delivery, while the most prevalent were non-payment/non-delivery, extortion, and personal data breach.

FBI reports the IC3 received 351,936 complaints in 2018—an average of more than 900 every day. The most frequently reported complaints were for non-payment/non-delivery scams, extortion, and personal data breaches. The most financially costly complaints involved [business email compromise](#), [romance or confidence fraud](#), and investment scams, which can include Ponzi and pyramid schemes.

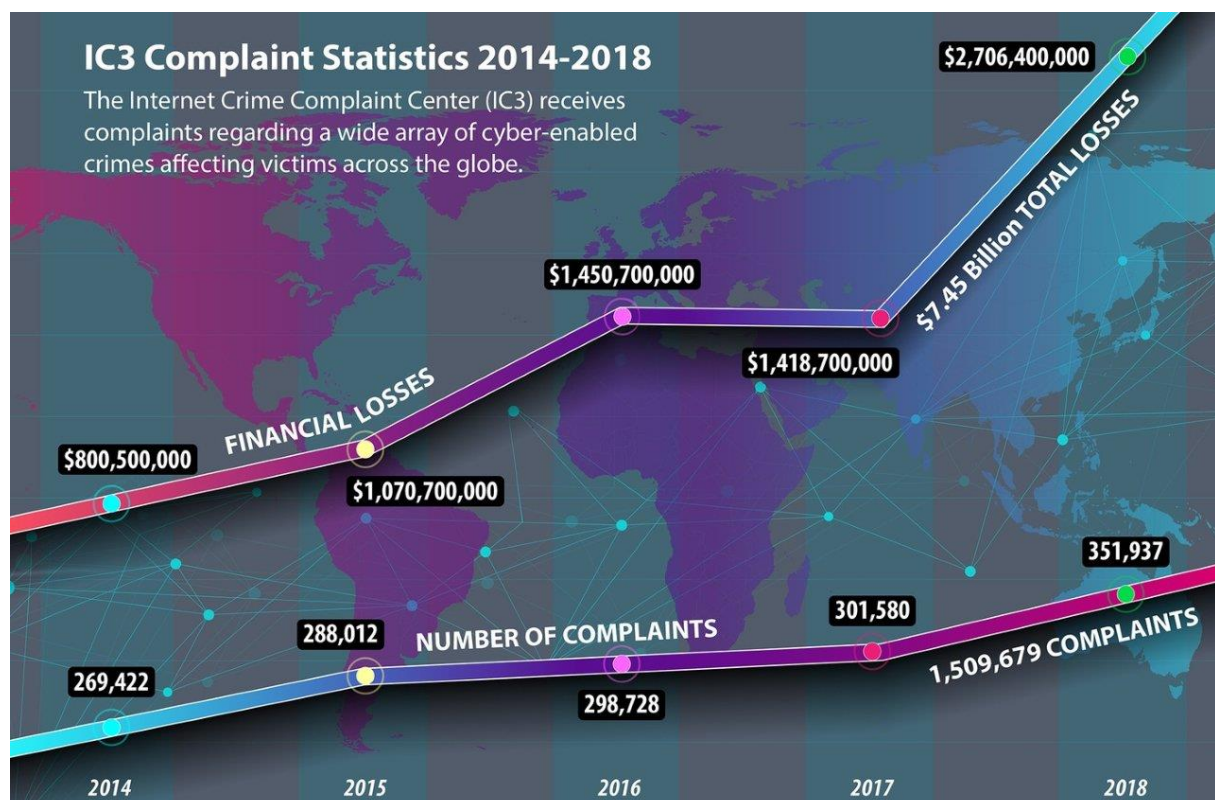


Figure 17. IC3 Complaint Statistics 2014-2018

The IC3 also states that its Recovery Asset Team (RAT) established in February 2018 was able to help cybercrime victims recover a large part of the funds lost due to various types of Internet crimes.

Through Domestic Financial Fraud Kill Chain (DFFKC) fraudulent fund recovery actions, the IC3 RAT "notified 56 field offices and 12 Legal Attachés of 1,061 DFFKC's totaling \$257,096,992, a recovery rate of 75%."

"The 2018 report shows how prevalent these crimes are," said IC3 chief Donna Gregory. "It also shows that the financial toll is substantial and a victim can be anyone who uses a connected device. Awareness is one powerful tool in efforts to combat and prevent these crimes. Reporting is another. The more information that comes into the IC3, the better law enforcement is able to respond."

BEC scams are the most profitable for crooks

Last year's cybercrime with the highest reported total losses, BEC (Business Email Compromise) — also known as EAC (Email Account Compromise) — reached a staggering \$1.2 billion in losses by targeting the wire transfer payments of both businesses and individuals.

"The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds," says the report.

BEC/EAC scams are the most popular method used by crooks to quickly make bank, given that most times it doesn't require that much skill because it relies on tricking people into wiring money to entities they already trust and whose bank accounts were switched with ones controlled by the criminals prior to the attacks.

IC3's findings are also confirmed by Proofpoint researchers, with Rob Holmes VP of email security at Proofpoint saying that "the frequency with which companies were targeted with email impersonation attacks tripled in 2018 relative to 2017 and increased greatly in sophistication. Adding to this global financial impact, it is worth noting that each year many incidents of this nature typically go underreported or unreported for various reasons."

As explained by the IC3, "Through the years, the scam has seen personal emails compromised, vendor emails compromised, spoofed lawyer email accounts, requests for W-2 information, and the targeting of the real estate sector."

2018 CRIME TYPES

By Victim Count				By Victim Loss			
Crime Type	Victims	Crime Type	Victims	Crime Type	Loss	Crime Type	Loss
Non-Payment/Non-Delivery	65,116	Other	10,826	BEC/EAC	\$1,297,803,489	Tech Support	\$38,697,026
Extortion	51,146	Lottery/Sweepstakes	7,146	Confidence Fraud/Romance	\$362,500,761	Harassment/Threats of Violence	\$21,903,829
Personal Data Breach	50,642	Misrepresentation	5,959	Investment	\$252,955,320	Misrepresentation	\$20,000,713
No Lead Value	36,936	Investment	3,693	Non-Payment/Non-Delivery	\$183,826,809	IPR/Copyright and Counterfeit	\$15,802,011
Phishing/Vishing/Smishing/Pharming	26,379	Malware/Scareware/Virus	2,811	Real Estate/Rental	\$149,458,114	Civil Matter	\$15,172,692
BEC/EAC	20,373	Corporate Data Breach	2,480	Personal Data Breach	\$148,892,403	Malware/Scareware/Virus	\$7,411,651
Confidence Fraud/Romance	18,493	IPR/Copyright and Counterfeit	2,249	Corporate Data Breach	\$117,711,989	Health Care Related	\$4,474,792
Harassment/Threats of Violence	18,415	Denial of Service/TDoS	1,799	Identity Theft	\$100,429,691	Ransomware	*\$3,621,857
Advanced Fee	16,362	Ransomware	1,493	Advanced Fee	\$92,271,682	Denial of Service/TDoS	\$2,052,340
Identity Theft	16,128	Crimes Against Children	1,394	Credit Card Fraud	\$88,991,436	Re-Shipping	\$1,684,179
Spoofing	15,569	Re-shipping	907	Extortion	\$83,357,901	Charity	\$1,006,379
Overpayment	15,512	Civil Matter	768	Spoofing	\$70,000,248	Gambling	\$926,953
Credit Card Fraud	15,210	Charity	493	Government Impersonation	\$64,211,765	Crimes Against Children	\$265,996
Employment	14,979	Health Care Related	337	Other	\$63,126,929	Hacktivist	\$77,612
Tech Support	14,408	Gambling	181	Lottery/Sweepstakes	\$60,214,814	Terrorism	\$10,193
Real Estate/Rental	11,300	Terrorism	120	Overpayment	\$53,225,507	No Lead Value	\$0.00
Government Impersonation	10,978	Hacktivist	77	Phishing/Vishing/Smishing/Pharming	\$48,241,748		
				Employment	\$45,487,120		

Descriptors*		
Social Media	40,198	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	36,477	

Descriptors*		
Social Media	\$101,045,973	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	\$182,106,976	

Figure 18. IC3 statistic of crime types in 2018.

FBI's IC3 also reported increased tech support fraud activity during 2018, with 14,408 recorded complaints and losses of roughly \$39 million, representing an increased of 161% when compared to the losses reported during 2017.

The common factor for the vast majority of tech support fraud reports is the fact that the victims are over 60 years of age, a devious yet logical approach showing that the crooks behind them really know their target "audience."

The IC3 also states that it "received 51,146 extortion-related complaints with adjusted losses of over \$83 million which represents a 242% increase in extortion related complaints from 2017."

As defined by the FBI, extortion will be used by cybercriminals as the last stage in "Denial of Service attacks, hitman schemes, sextortion, government impersonation schemes, loan schemes, and high-profile data breaches."

"It is critical that organizations prioritize a people-centric approach to security that protects all parties (their employees, customers, and business partners) against phishing, email fraud, credential theft, and brute force attacks," also said Holmes. "We also recommend layered defenses at the network edge, email gateway, in the cloud, and endpoint, along with strong user education to provide the best defense against these types of attacks."

Source: <https://www.bleepingcomputer.com/news/security/cybercrimes-total-earnings-skyrocketed-to-27-billion-says-the-fbi/>

11. Over 500% Increase in Ransomware Attacks Against Businesses

Cybercriminals have started focusing their efforts on businesses during Q1 2019, with consumer threat detections decreasing by roughly 24% year over year while businesses have seen a 235% increase in the number of cyber attacks against their computing systems.

For consumers, the number of detections for Trojans and RiskwareTool malware families has kept going down since Q1 2018 and backdoors, spyware, and MachineLearning/Anomalous malware have seen increases of 85%, 95%, and 221% respectively.

On the other hand, when it comes to the malware families detected in corporate environments, Malwarebytes' "Cybercrime Tactics and Techniques Q1 2019" report shows skyrocketing detection rate all across the board since Q1 2018, while hijackers were the only malware that continued to show up less and less during the last year.

Consumer Detections					Business Detections				
Q1 2019	Category	Threat Count	Q4 2018 %	Q1 2018 %	Q1 2019	Malware Category	Threat Count	Q4 2018 %	Q1 2018 %
1	Adware	15,283,211	-26%	12%	1	Trojan	4,703,567	222%	649%
2	Generic	10,269,367	32%	4%	2	Generic	1,039,442	-18%	111%
3	Trojan	9,886,157	-61%	-34%	3	Adware	954,674	153%	375%
4	RiskwareTool	4,076,250	-32%	-67%	4	MachineLearning/Anomalous	895,699	147%	NEW
5	Backdoor	2,278,733	-65%	85%	5	Backdoor	475,314	-80%	485%
6	MachineLearning/Anomalous	1,710,503	-21%	221%	6	RiskwareTool	389,357	45%	56%
7	HackTool	1,543,912	1%	18%	7	Ransom	336,634	189%	508%
8	MisplacedCertificate	1,214,708	New	New	8	Malware	263,035	NEW	NEW
9	OSX	1,187,836	30%	New	9	Hijacker	91,466	-73%	-69%
10	Spyware	761,510	-11%	95%	10	Exploit	76,784	76%	NEW

Figure 19. Malware detection (by family) in consumer and in business environments

Out of all malware families impacting commercial entities, ransomware has seen huge comeback with increases of 189% since Q4 2018 and a massive 508% uptick since Q1 2018, while on the consumer side ransomware was "knocked out of the top 10 from its previous steady ranking for several years running."

As detailed by Malwarebytes, this huge increase in corporate ransomware detections happened "thanks in large part to a massive attack by the Trolldesh ransomware against US organizations in early Q1."

This trend is also backed by FBI's Internet Crime Complaint Center (IC3) annual Internet Crime Reports ([2013](#), [2014](#), [2015](#), [2016](#), [2017](#), [2018](#)) which show that while ransomware has definitely seen a decrease in the number of incidents since 2016, the total losses have increased despite a decreasing number of complaints. A detailed overview of the number of yearly ransomware complaint and total losses as reported by the IC3 is available in the table below.

Year	Complaints	Total Losses
2013	991	\$539,562.00
2014	1402	\$490,577.00
2015	2453	\$1,620,814.00
2016	2673	\$2,431,261.00
2017	1783	\$2,344,365.00
2018	1394	\$3,621,857.00

Figure 20. Ransomware complaints compared to total losses between 2013-2018

Even though it might not be immediately obvious, this happened because cybercriminals have switched their targets from home users to commercial organizations which can afford to pay larger ransoms to have their computing systems unlocked and files decrypted. The [2018 edition of IC3's Internet Crime Report](#) also underlined that not all ransomware victims report the incident, thus leading to an "artificially low ransomware loss rate."

Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, equipment, or any third party remediation services acquired by a victim. In some cases victims do not report any loss amount to the FBI, thereby creating an artificially low ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.

The Malwarebytes report conclusions are the result of combining statistics and intel collected between January 1 and March 31, 2019. They rely on data from the company's "Intelligence, Research, and Data Science teams" with telemetry added to the mix from both the "consumer and business products on the PC, Mac, and mobile devices."

More details on the evolution of other threats targeting consumers and businesses are available in Malwarebytes' full [Cybercrime Tactics and Techniques \(CTNT\) Report](#).

Source: <https://www.bleepingcomputer.com/news/security/over-500-percent-increase-in-ransomware-attacks-against-businesses/>

12. Zero Trust: Why Your Most Privileged Users Could Be Your Biggest Security Weakness

Your security infrastructure is there to protect your organization from malicious threats. That much is obvious, but what happens when a user's credentials are compromised and threat actors access your systems? This could expose your company to a data breach and all the reputational damage, operational downtime and financial costs that come with it.

But all access is not created equal. What would happen to your organization if one of your privileged users had their identity compromised? [Privileged account management \(PAM\)](#) helps protect against the most dangerous data breaches because it enables you to closely monitor your most sensitive accounts.

Protecting Your Privileged Users Is Paramount

The majority of security breaches involve the compromise of user and privileged accounts via attack vectors such as phishing, malware and other means. Once the attacker establishes a foothold in the network, the next step is to find and hijack a privileged account, enabling the actor to move laterally across the network while appearing as a legitimate user.

At this point, the malicious activity can begin. Attackers often search compromised networks for valuable data such as personally identifiable information (PII), intellectual property and financial data. Such sensitive information enables threat actors to commit financial fraud as well as other crimes.

The bottom line is that protecting critical data means protecting your most valuable users. That's why Gartner recognized privileged account management in its "[Top 10 Security Projects for 2019](#)," along with detection and response, cloud security posture management, business email compromise, and more. The research firm also placed PAM on its 2018 list.

Further demonstrating the criticality of PAM is a [Centrify](#) survey that revealed 74 percent of data breaches involve unauthorized access to a privileged account. If privileged access is the most fruitful point of attack for cybercriminals, why are so many companies still not taking even basic steps to prevent this abuse?

Tackle Privileged Abuse With the Zero Trust Model

If you're looking to tackle privileged abuse once and for all, you should consider adopting a [zero trust strategy](#). According to [Forbes](#), applying an approach of "never trust, always verify" can help grow digital business models. To implement a zero trust architecture, you must adopt a strategy built around constant verification. This means creating an environment in which all access is cut off until the network knows who is attempting to access it.

Since cybercriminals target privileged users, consider abandoning the traditional castle-and-moat approach and limit the user's ability to move through internal systems once they

have initially accessed the network. Default connections within your network are a key point of failure that malicious agents are constantly trying to exploit.

Traditional firewalls act as a barrier between internal and external activity. To move to a zero trust environment, you must create a more granular perimeter around individually segmented applications, databases and other key pieces of your infrastructure.

The first step is to define your strategy, not your technology. Decide how you want to proceed, examine how you can apply this to your organization's infrastructure and then look for the right tools to execute that approach.

It's all about building a system that can [protect the most valuable users and systems](#) within your organization. Understand that your privileged users are also the ones that make your company the most vulnerable — that is, if you don't mitigate those risks by monitoring these accounts differently. Creating a verification-centric security system for these users is one way to reduce the biggest risks.

[Register for the webinar to learn more](#)

Source: <https://securityintelligence.com/posts/zero-trust-why-your-most-privileged-users-could-be-your-biggest-security-weakness/>

13. Old Vulnerabilities Are Still Good Tricks for Today's Attacks

The value of a security vulnerability drops significantly the moment it gets patched but the bad guys will keep exploiting it for as long as they can find victims that are worth the effort.

According to a report today, the most exploited security bugs in the first quarter of 2019 were well-known, old problems, some of them patched almost a decade ago. Statistics and research from Fidelis Cybersecurity show that about a third of the alerts recorded by the company were for exploits, vulnerabilities, and malware that emerged in 2017 and earlier. The malware-generated events that caused most alerts pointed to [H-W0rm](#) and njRAT, two remote access tools (RATs) that have been in use since at least 2012.

Events of Interest Q1 2019

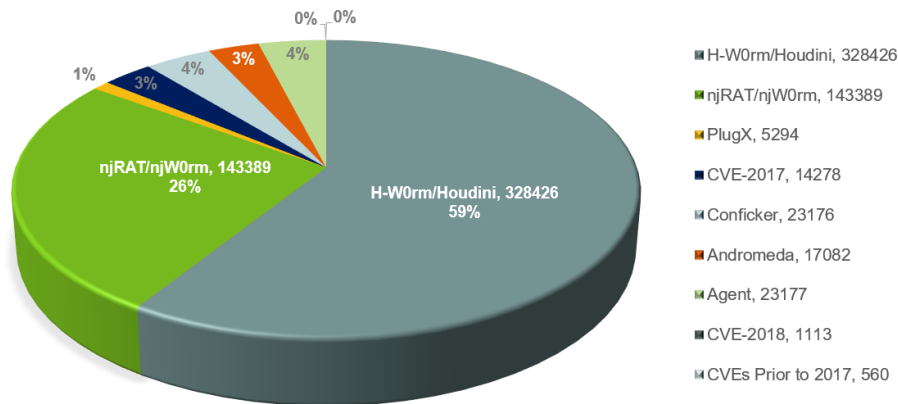


Figure 21. Malware of Interest Q1 2019

njRAT is customizable and there are numerous tutorials explaining how to use it; some go as far back as 2012 and are extremely easy to find. This clarifies why it is so popular. Fidelis researchers believe that the authors of the two threats may be working together, based on observations from forums on the dark web.

Apart from old tools and kits, the researchers also noticed that 27% of the compromise attempts and alerts were for vulnerabilities from 2017 and earlier. The most prevalent are the following:

- [CVE-2017-8570](#) - "Composite Moniker" remote code execution, exploit code available
- [CVE-2017-0143](#) - affects SMBv1 protocol, exploit released by the ShadowBrokers (Eternal Synergy)
- [CVE-2018-11776](#) - remote code execution in Apache Struts, exploit available
- [CVE-2017-11882](#) - remote code execution in Microsoft Office, exploit available
- [CVE-2009-3129](#) - remote code execution in Microsoft Excel/Word used in operation "[Red October](#)" exploit available

It is not surprising that the vulnerabilities above are leveraged in cyber attacks since there are public exploits for all of them. The disquieting thing about this is that after all this time there are still unpatched machines belonging to victims that are worth the trouble of hacking. Old security bugs and malware kits made for about 27% of the detections Fidelis recorded in Q1 2019. This amounts to more than 550,000 incidents investigated.

Fidelis Total Detections Q1 2019

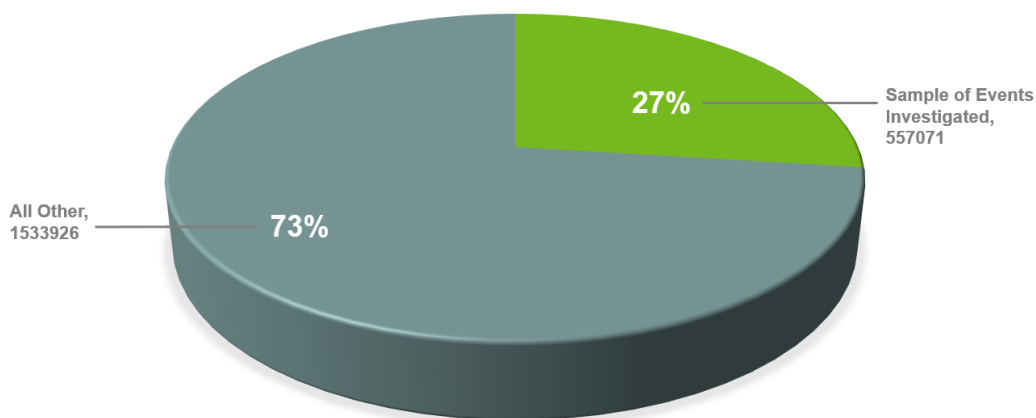


Figure 22. Fidelis Detections Q1 2019

Source: <https://www.bleepingcomputer.com/news/security/old-vulnerabilities-are-still-good-tricks-for-todays-attacks/>

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.

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

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