



Advanced Security Operations Center  
Telelink Business Services  
[www.telelink.com](http://www.telelink.com)

# Monthly Security Bulletin

June 2019

## Table of Contents:

Executive Summary.....	2
1. Over 275 Million Records Exposed by Unsecured MongoDB Database.....	5
2. Hackers Selling Access and Source code from Antivirus Companies.....	7
3. Crypto-Mining Hacking Groups Wage War in the Cloud.....	10
4. ThreatList: Top 5 Most Dangerous Attachment Types.....	13
5. Tales From the SOC: Hunting for Persistent Malware.....	17
6. Two More Windows 10 Zero-Day PoC Exploits Released, Brings Total to 4.....	21
7. Calibration Attack Drills Down on iPhone, Pixel Users.....	24
8. Android Users Being Spammed Using Fake Missed Call Alerts.....	27
9. Snapchat Privacy Blunder Piques Concerns About Insider Threats.....	29
10. macOS Unpatched for Executing Untrusted Code off the Network.....	30
11. Malspam Campaigns Use HawkEye Keylogger to Target Businesses.....	32



## Executive Summary

1. "A huge MongoDB database exposing 275,265,298 records of Indian citizens containing detailed personally identifiable information (PII) was left unprotected on the Internet for more than two weeks." To learn more [Jump to article.](#)
2. Hacking group specialized in targeting corporate and government networks across the globe sells "access to the networks of at least three antivirus companies in the U.S. and source code for their software products." To learn more [Jump to article.](#)
3. "Two hacking groups connected to large-scale malicious crypto-mining campaigns have been targeting each other's cryptominers as part of an ongoing battle to get control of vulnerable cloud-based infrastructure." To learn more [Jump to article.](#)
4. What are the biggest attachment scams trending on a wide scale in 2019? From "ZIP attachments spreading Gandcrab, to DOC files distributing Trickbot" malicious actors are reining campaigns to spread spam. To learn more [Jump to article.](#)
5. How the SOC are hunting for persistent malware? Find the steps of cracking down on the threats. To learn more [Jump to article.](#)
6. „After releasing exploit code for three zero-day vulnerabilities in Windows 10 over the past 48 hours“, SandboxEscaper security researcher and exploit developer has published another one totaling the exploits to 4. To learn more [Jump to article.](#)
7. "A new way of tracking mobile users creates a globally unique device fingerprint that browsers and other protections can't stop." The new privacy attack uses Apple iPhone sensors to create a skeleton fingerprint globally unique for any given mobile user. Furthermore, this has implications not only for iPhone users but for Google Pixels phones which run on Android. To learn more [Jump to article.](#)
8. "Scammers are abusing the Notifications and Push APIs and Google Chrome on Android devices to push spam alerts customized to look like a missed phone call." The sole purpose of this is to reengage the user in a way that looks normal for the native app. To learn more [Jump to article.](#)
9. "Snap, the company behind the popular Snapchat social media app, has found itself in hot water after a recent report revealed that Snap employees were abusing their access to private user data – which includes location data, saved Snaps and phone numbers.". The way they did is by using the SnapLion tool, initially built for law enforcement purposes, which the employees for their own purposes. To learn more [Jump to article.](#)
10. "Details have been released for an unpatched vulnerability in macOS 10.14.5 (Mojave) and below that allows a hacker to execute arbitrary code without user interaction. By leveraging the flaw it is possible to bypass Gatekeeper, the built-in defense in macOS that guards the operating system against running untrusted applications. Gatekeeper achieves this by verifying the code signing certificate obtained through Apple's developer program." To learn more [Jump to article.](#)
11. For the last couple of months IBM's X-Force has observed a massive worldwide attack campaign targeting businesses with the HawkEye keylogger malware using span servers located in Estonia sending malicious emails posing as Spanish banks. To learn more [Jump to article.](#)

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

## 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 inside and outside visibility, deep attack 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					
Attack 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 in Lite)

Advanced Plan  
(incl. all in Prof)

## 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

<https://www.telelink.com/asoc/>

# 1. Over 275 Million Records Exposed by Unsecured MongoDB Database

A huge MongoDB database exposing 275,265,298 records of Indian citizens containing detailed personally identifiable information (PII) was left unprotected on the Internet for more than two weeks.

Security Discovery researcher Bob Diachenko discovered the publicly accessible MongoDB database hosted on Amazon AWS using Shodan, and as historical data provided by the platform showed, the huge cache of PII data was first indexed on April 23, 2019.

As he found out after further investigation, the exposed data included information such as name, gender, date of birth, email, mobile phone number, education details, professional info (employer, employment history, skills, functional area), and current salary for each of the database records.

```
"_id" : ObjectId("5cbf0fd076da82177d173910"),
"Course(2nd Highest Education)" : NaN,
"Name" : "██████████",
"Current Location" : "██████████",
"Industry" : "Catering/Food Services/Restaurant, Hotel/Travel/Tourism/Airlines/Hospitality",
"Institute(Highest Education)" : "Others",
"Specialization(2nd Highest Education)" : NaN,
"Resume Id" : "██████████",
"Specialization(Highest Education)" : "Other B.A.",
"Current Employer" : "██████████",
"Mobile No" : "9██████████",
"Preferred Location" : "Anywhere in India",
"Course(Highest Education)" : "B.A.",
"Key Skills" : "GPs, PNL, stocks, quest care, staff development and training, IT skills, gener",
"Previous Employer" : "██████████",
"Date of Birth" : "1986-04-14 00:00:00",
"Address" : "██████████",
"Area of Specialization" : "Food & Beverage, Guest Relation, Restaurant",
"Institute(2nd Highest Education)" : NaN,
"Resume Title" : "f&b operational expert and has got graduation from london",
"Current Salary" : "6,00,000 annually",
"Email Id" : "██████████@yahoo.com",
"Gender" : "Male",
"Level" : "Others",
"Functional Area" : "Hotel/Restaurant",
"Alternate Number" : "██████████"
```

*Figure 1. Sample database record*

While the unprotected MongoDB database leaked the sensitive information of hundreds of millions of Indians, Diachenko did not find any information that would link it to a specific owner.

Additionally, the names of the data collections stored within the database suggested that the entire cache of resumes was collected "as part of a massive scraping operation" for unknown purposes.

Collection Statistics

_id	Collection	Count	Size	Storage Size	Avg Object Size	Indexes	Index Size	Padding
	mediafire_csv_last_final	275265298	110.0 GiB (118,0...	114.6 GiB (123,0...	428 B (428)	1	8.3 GiB (8,942,7...	1.0
	mediafire_csv_4	33279137	12.1 GiB (13,02...	12.7 GiB (13,59...	391 B (391)	1	1.0 GiB (1,080,6...	1.0
	mediafire_csv_final_2	4250988	1.9 GiB (2,092,6...	2.6 GiB (2,828,7...	492 B (492)	1	133.1 MiB (139,...	1.0
	mediafire_csv_2	1945618	1.1 GiB (1,132,6...	1.1 GiB (1,164,9...	582 B (582)	1	60.2 MiB (63,14...	1.0
	mediafire_csv	1459614	152.4 MiB (159,...	232.0 MiB (243,...	109 B (109)	1	45.2 MiB (47,37...	1.0
	mediafire_csv_final_3	339894	229.3 MiB (240,...	320.3 MiB (335,...	707 B (707)	1	10.5 MiB (11,04...	1.0
	jalandhar	20000	9.4 MiB (9,821,4...	10.7 MiB (11,18...	491 B (491)	1	638.8 KiB (654,...	1.0
	daman	4638	8.0 MiB (8,375,8...	10.7 MiB (11,18...	1.8 KiB (1,805)	1	159.7 KiB (163,...	1.0
	mediafire_csv_final_1	3426	8.8 MiB (9,178,8...	10.7 MiB (11,18...	2.6 KiB (2,679)	1	119.8 KiB (122,...	1.0
	mediafire_csv_final_4	2374	7.7 MiB (8,097,9...	10.7 MiB (11,18...	3.3 KiB (3,411)	1	87.8 KiB (89,936)	1.0
	mediafire_csv_3	585	28.1 KiB (28,736)	40.0 KiB (40,960)	49 B (49)	1	31.9 KiB (32,704)	1.0
	my_collection_keys	585	28.1 KiB (28,736)	40.0 KiB (40,960)	49 B (49)	1	31.9 KiB (32,704)	1.0
	mediafire_csv_final	484	102.2 KiB (104,...	168.0 KiB (172,...	216 B (216)	1	24.0 KiB (24,528)	1.0
	Medical_test	297	296.4 KiB (303,...	680.0 KiB (696,...	1021 B (1,021)	1	24.0 KiB (24,528)	1.0
	system.indexes	17	1.9 KiB (1,904)	8.0 KiB (8,192)	112 B (112)	0	0 B (0)	1.0
	yeppi	2	96 B (96)	8.0 KiB (8,192)	48 B (48)	1	8.0 KiB (8,176)	1.0
	test_collect111ion	2	96 B (96)	8.0 KiB (8,192)	48 B (48)	1	8.0 KiB (8,176)	1.0
	test_collection	2	96 B (96)	8.0 KiB (8,192)	48 B (48)	1	8.0 KiB (8,176)	1.0

Figure 2. Exposed database contents

The researcher "immediately notified Indian CERT team on the incident, however, database remained open and searchable until today, May 8th, when it got dropped by hackers known as 'Unistellar' group."

After the database got dropped by the hackers, Diachenko discovered the following message left behind after deleting all the data:

```

1 {
2   "_id" : ObjectId("5cd1dd4ca4baec3fb04d24a2"),
3   "key" : "4015bc9ee91e437d90df83fb64fbbe312d9c9f05",
4   "database" : "admin",
5   "message" : "Restore ? Contact : unistellar@hotmail.com"
6 }
7 // -----
8 {
9   "_id" : ObjectId("5cd1dd5117c33f4df2e117f4"),
0   "key" : "c3399aa786fc87807670aa291f07cfac999635a",
1   "database" : "mediafire_csv_last_final",
2   "message" : "Restore ? Contact : unistellar@hotmail.com"
3 }
4 // -----
5 {
6   "_id" : ObjectId("5cd1dd526a60e35dee71aa34"),
7   "key" : "5a9b181f58cbce1450c74d07918b188b712610b6",
8   "database" : "local",
9   "message" : "Restore ? Contact : unistellar@hotmail.com"
0 }
1 // -----
2 {
3   "_id" : ObjectId("5cd1dd55ef08e1e42212cd0f"),
4   "key" : "4e1243bd22c66e76c2ba9eddc1f91394e57f9f83",
5   "database" : "test",
6   "message" : "Restore ? Contact : unistellar@hotmail.com"
7 }
8

```

Figure 3. The message left by the hackers

Diachenko found multiple other unsecured databases and servers, unearthing a publicly accessible 140+ GB MongoDB database containing a huge collection of 808,539,939 email records during Early-March and another one with over 200 million records with resumes from Chinese job seekers in January.

He was also the one who discovered the personal information of more than 66 million individuals left out in the open on the Internet during December and an extra 11 million

records during September, with all of them being stored in misconfigured and passwordless MongoDB instances.

These data leaks are a thing because a lot of MongoDB databases are left publicly accessible by their owners and are not properly secured. This means that they can be blocked by securing the database instance.

MongoDB provides a Security section on the Documentation website which shows how to properly secure a MongoDB database, as well as a security checklist for MongoDB administrators.

Source: <https://www.bleepingcomputer.com/news/security/over-275-million-records-exposed-by-unsecured-mongodb-database/>

## 2. Hackers Selling Access and Source code from Antivirus Companies

A hacking group or individual is advertising access to the networks of at least three antivirus companies in the U.S. and source code for their software products.

The initial asking price was \$250,000 for access information and \$150,000 for the source code but they were ready to sell both for at least \$300,000 depending on the antivirus company the buyer is interested.

This offer was for each individual company and it is not a set price. It could go as high as \$1 million for one access. A definitive offer is still being discussed with intermediaries.

### Claiming 30 terabytes of stolen data

In March, an actor calling themselves Fxmsp announced to members of criminal underground communities that they could provide exclusive information stolen from major antivirus companies located in the U.S.

In late April, Fxmsp said that after hard work through the first quarter of 2019 they managed to breach the companies' networks and had secure long-term access.

They offered screenshots of folders that supposedly contained 30 terabytes of data, claiming it was extracted from the breached networks.



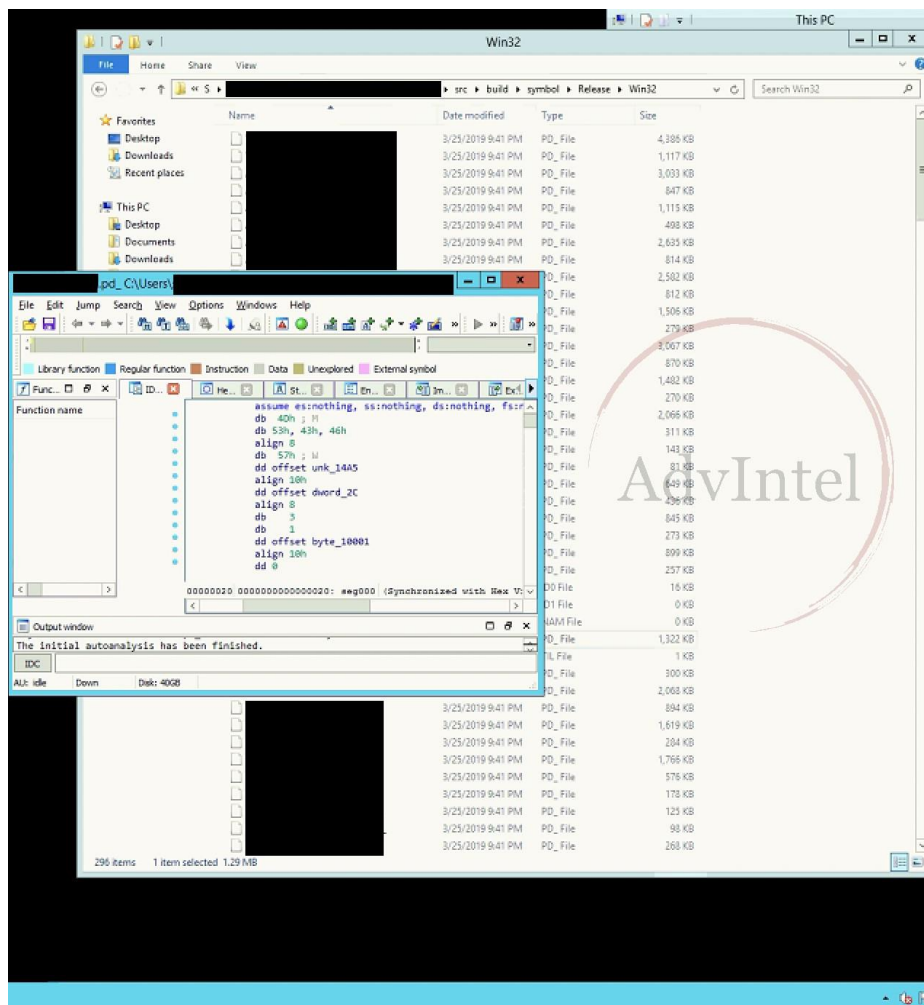


Figure 4.

"The folders seem to contain information about the company's development documentation, artificial intelligence model, web security software, and antivirus software base code," security company AdvIntel says in a report released today.

Yelisey Boguslavskiy, AdvIntel's director of security research, told BleepingComputer that Fxmsp reportedly compromised the Active Directory (AD) of at least one company and established persistence through an external Remote Desktop Protocol (RDP) server.

AD is the most critical part of a Windows network, as the server is responsible for authenticating and authorizing all users and computers on the network; it is also where security policies are defined for all the systems it manages.

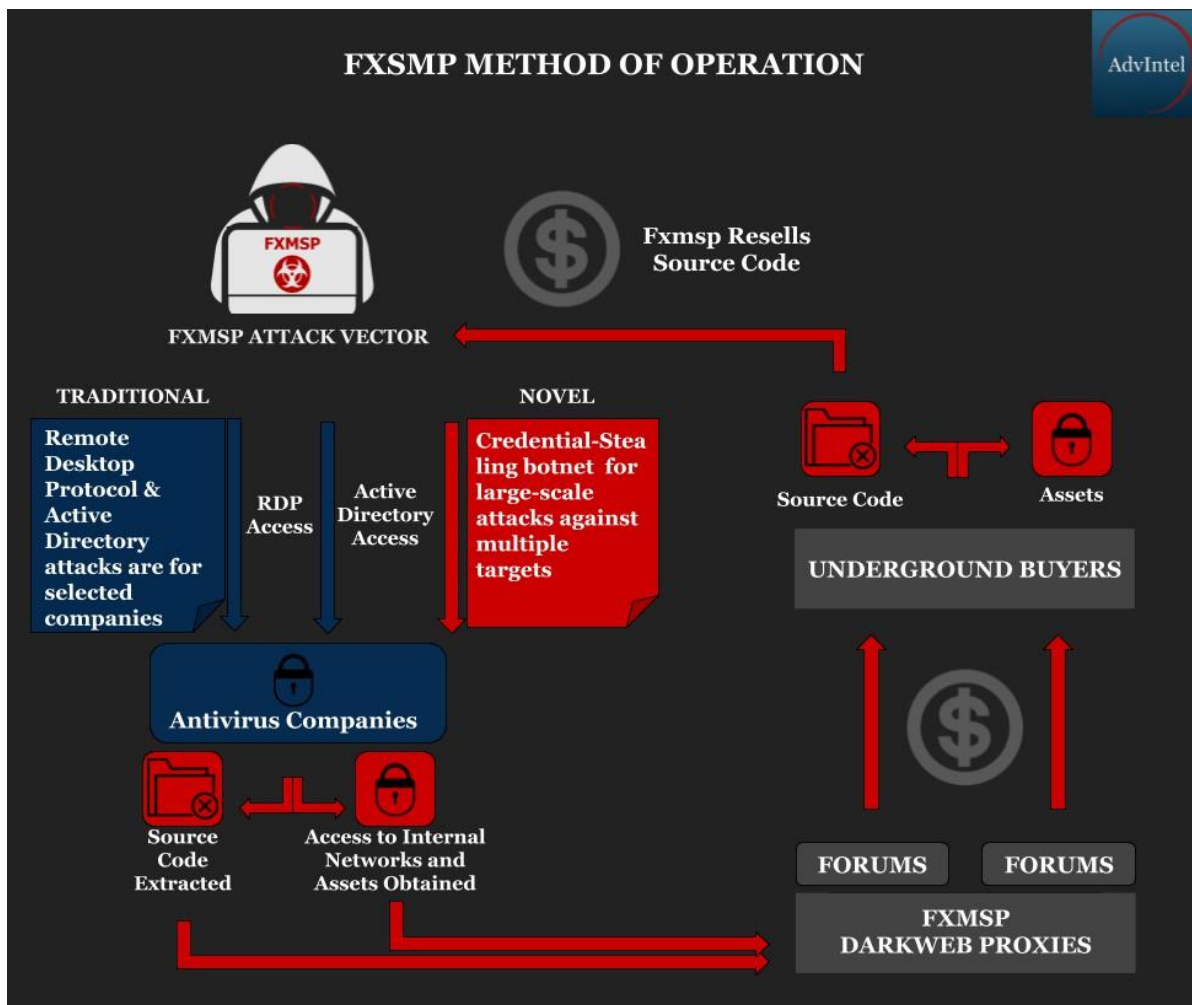


Figure 5.

This tactic has been used by the Carbanak gang against banks across the world. It was discovered by Kaspersky threat researchers at a bank in Russia.

According to Boguslavskiy, Fxmsp named three of its victims and claimed that they had compromised a fourth antivirus firm, but did not disclose its name.

### Actor goes dark, resurfaces with goody bag

"The actor claimed that antivirus breach research has been their main project over the last six months, which directly correlates with the six-month period during which they were silent on the underground forums where they normally post," says AdvIntel.

According to the New York-based fraud prevention company, Fxmsp disappeared from underground forums in October 2018 and returned in April this year.

Fxmsp appears to be a hacker group that speaks both Russian and English. They are specialized in targeting corporate and government networks across the globe. In a post in February 2018 we found on an underground forum, the actor advertised access to the

corporate networks of a company, which included account entries for all employees, "from cleaners to the president."

Monetizing access data is done via proxy sellers that attract buyers from both Russian and English criminal forums. Although they sell only to one buyer, Boguslavskiy told us that Fxmsp is known for secretly re-selling their "goods."

The activity of the individual(s) behind the Fxmsp alias is known among infosec experts. FireEye mentioned them in its 2018 e-crimes report for the EMEA (Europe, the Middle East, and Africa) region.

On April 5, 2018, Fxmsp advertised access information for the network of a hotel chain with locations in Europe, Africa, and South America.

AdvIntel believes that Fxmsp is a credible hacker collective that sells verifiable corporate access. The researchers believe that the group turned a profit of about \$1 million by now. Other offers from Fxmsp include network access for the following businesses:

- Keystone Bank Limited
- Key Family of Companies
- DeltaWestern Petroleum
- Peckar & Abramson, P.C. (US Legal Company)
- Blue Stone Capital Investments LLC (US Investment Company)
- Reliance Industries Limited (Indian Industrial Holding)
- Ghana Ministry of Finances Database
- Bogota Electronic Government Database

The actor seems to be active since at least 2017 and assumed a stolen identity of someone named Andrey Turchin to carry out their business. We were told by someone with knowledge about this actor that this identity is that of a real person. Although it is burned at the moment, this shows the level of sophistication this actor has.

*Source:* <https://www.bleepingcomputer.com/news/security/hackers-selling-access-and-source-code-from-antivirus-companies/>

### 3. Crypto-Mining Hacking Groups Wage War in the Cloud

Two hacking groups connected to large-scale malicious crypto-mining campaigns have been targeting each other's cryptominers as part of an ongoing battle to get control of vulnerable cloud-based infrastructure.

The first of the two crypto-mining (also known as cryptojacking) attackers is Pacha Group, a threat group of Chinese origins profiled by Intezer Labs while pushing a cryptocurrency mining malware named Linux.GreedyAntd and first detected during September 2018.

At the time, Intezer Labs' researchers discovered that the group's Linux.GreedyAntd malware is designed to hunt down other cryptojacking malware already present on the systems it manages to infect, a technique previously used by similar malware strains.

To drop their cryptomining malware, Pacha Group "launch a brute-force attack against services like WordPress or PhpMyAdmin, or used a known exploit for an outdated version of alike services," said Intezer Labs.

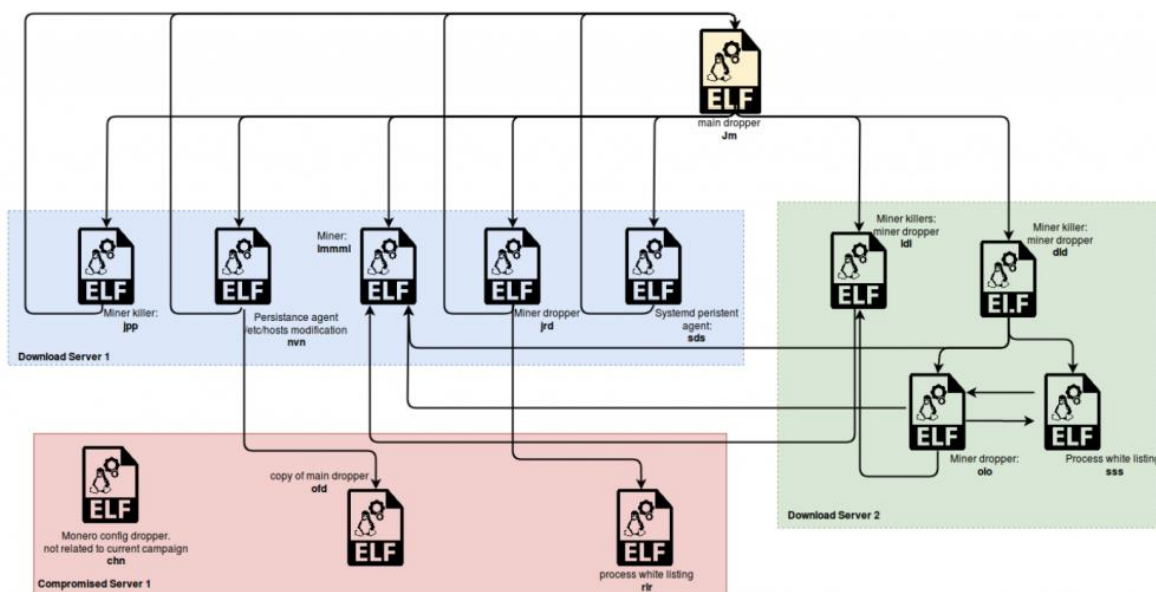


Figure 6. Linux.GreedyAntd malware architecture (Image: Intezer Labs)

## Cryptojacking malware under siege

Linux.GreedyAntd, a modular malware which uses Systemd gain persistence—unlike other strains which employ cron-job—to make itself harder to detect and remove is also used to attack and remove the cryptominers dropped by other cybercrime groups, with Rocke being the most prominent of them based on their extensive operations.

As Intezer Labs' tech analysis says "The main malware infrastructure appears to be identical to previous Pacha Group campaigns, although there is a distinguishable effort to detect and mitigate Rocke Group's implants."

The malware used by the Rocke group to surreptitiously mine for cryptocurrency in campaigns going as early as April 2018 also comes with a "kill list" which helps it find and shutdown any previously running cryptojacking malware.

On the other hand, Pacha Group has also added a list of hardcoded IP addresses to Linux.GreedyAntd's blacklist which will block Rocke's cryptominers by routing their traffic back to the compromised machines.

Both groups' malware strains come with shared capabilities like the ability to search for and to disable cloud security and monitoring products from vendors such as Tencent Cloud and



Alibaba Cloud, support for the Libprocesshider lightweight user-mode rootkit, as well as an exploit used to abuse an Atlassian vulnerability.

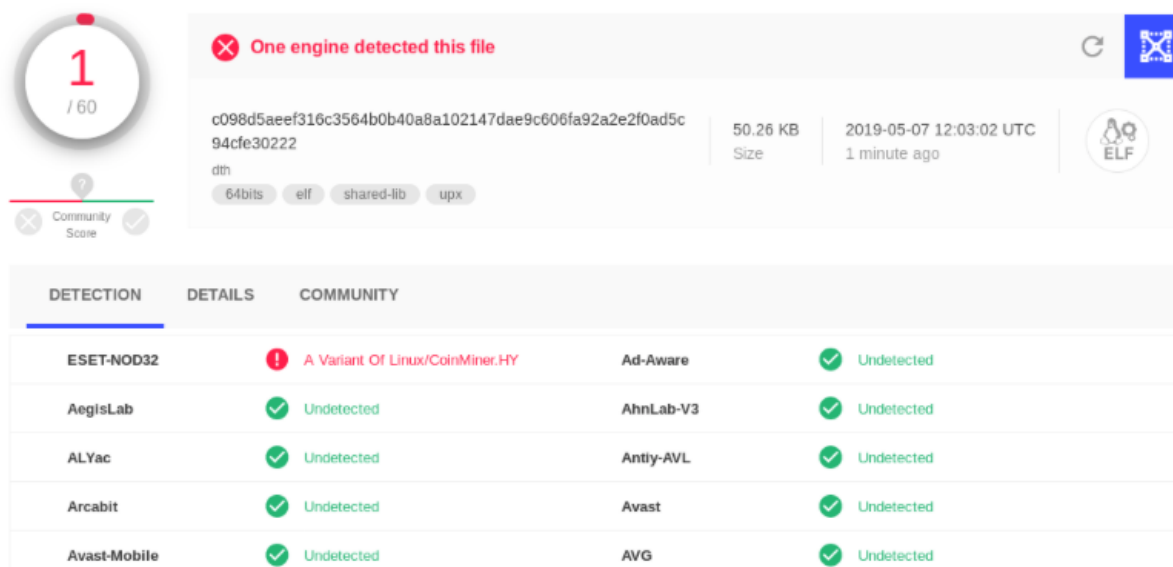


Figure 7. New Linux.GreedyAntd variant detection rate (Image: Intezer Labs)

### Cloud infrastructure increasingly targeted

With both groups actively targeting cloud infrastructure to run their cryptojacking campaigns using cloud computing power, a clash was bound to happen during their struggle to be the ones abusing vulnerable systems for their own profit.

"We believe that these findings are relevant within the context of raising awareness about cloud-native threats, particularly on vulnerable Linux servers," says Intezer Labs' report. "While threat actor groups are competing with one another, this evidence may suggest that threats to cloud infrastructure are increasing."

The report highlights Pacha Group's efforts to target its main competitor, the Rocke group, in the race to compromise and get control of the largest possible share of the cloud.

As previously reported by BleepingComputer, various crypto-mining groups have been switching their targets to Docker and Kubernetes systems as part of a larger push to abuse cloud computing resources, a push going as far as March 2018.

A list of Indicators of Compromise (IOCs) is provided by Intezer Labs at the end of their [full technical analysis](#).

Source: <https://www.bleepingcomputer.com/news/security/crypto-mining-hacking-groups-wage-war-in-the-cloud/>

## 4. ThreatList: Top 5 Most Dangerous Attachment Types

From ZIP attachments spreading Gandcrab, to DOC files distributing Trickbot, researchers tracked five widescale spam campaigns in 2019 that have made use of malicious attachments.

Researchers with F-Secure have tracked the top spam-related attachments and campaigns used so far in 2019. The verdict, ZIPs, PDF, and MS office files (such as DOC and XLSM file attachments) were more commonly used in huge spam campaigns than any other type attachment.

In addition, researchers noticed that disc image files (ISO or IMG files that store the content and structure of an entire disk, like a DVD or Blue-Ray) are increasingly being used to spread malware. This has been seen in a growing number of smaller campaigns distributing the AgentTesla malware and NanoCore remote access trojan, according to researchers.

“In February and March, we saw huge spam campaigns using ZIP files to send out GandCrab ransomware, and DOC and XLSM files to distribute Trickbot banking trojan,” researchers with F-Secure said in a post last week. “In the same time period, we saw a similarly large campaign targeting American Express [customers], and a ‘Winner’ scam, both using PDF file attachments.”

### **ZIP Files Spreading GandCrab**

Researchers said that in February and March, there were huge spam campaigns spreading the infamous GandCrab ransomware. These campaigns were using ZIP files, designed to appear to be sending a photo to someone.

However, in reality the ZIP file contains a obfuscated JavaScript downloader, which executes a PowerShell script that downloads and executes the GandCrab ransomware binary. If the payload is successfully downloaded and executed, it then encrypts the victim’s machine and displays a ransomware note (below).

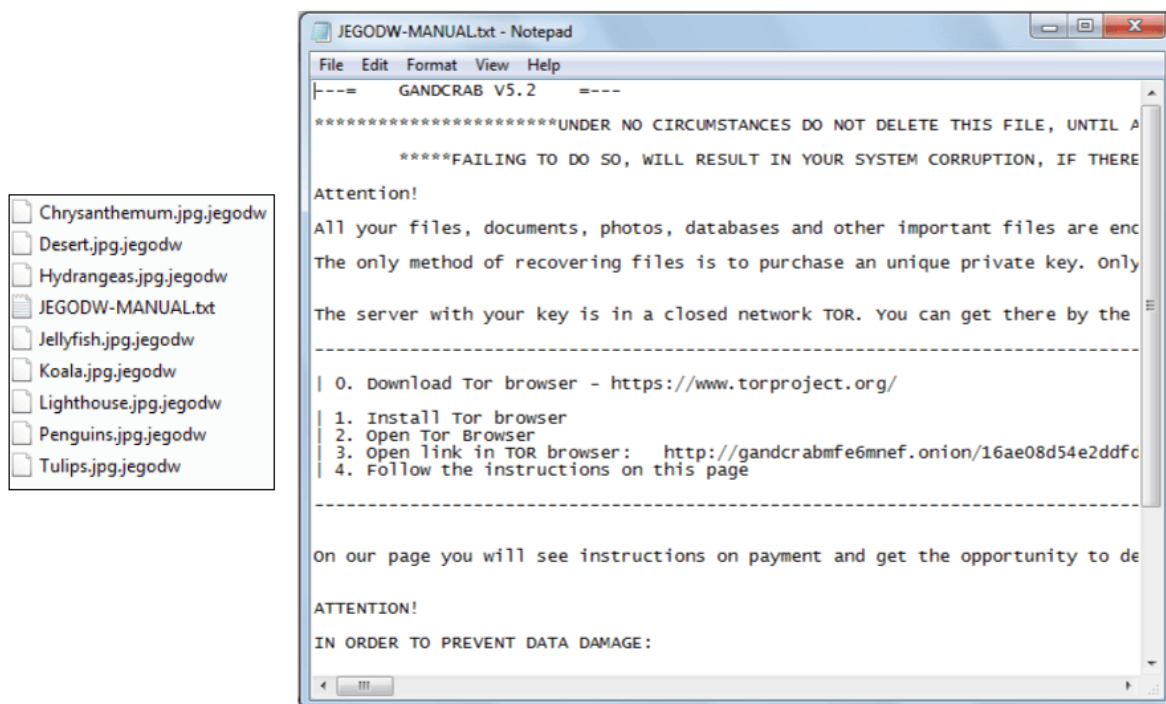


Figure 8.

### DOC/XLSM Files Delivering Trickbot

Researchers also noted huge spikes in tax-themed spam campaigns in March that were utilizing DOC and XLSM (macro-enabled spreadsheet created by Microsoft Excel) files to deliver the Trickbot modular banking trojan. The email in the campaign, which were purporting to feature tax billing records, contained office doc attachments with a malicious macro that downloads and executed the payload using a bitsadmin tool. BitsAdmin is a legitimate command-line tool that can be used to create download or upload jobs and monitor their progress.

Once downloaded and executed, the Trickbot sample starts execution and creates modules on the victim's machine, researchers said, stealing "as much data possible" – including banking credentials and more.

The TrickBot financial malware was first identified in 2016. Several recent campaigns demonstrate its fast-paced evolution by those behind its development. Researchers have noted the malware's new code-injection techniques, updated info-stealing module and a customized redirection method.

### PDF Files Used in Amex Phishing

Another popular spam campaign in March revolved around a phishing attack that was making use of PDF files to target American Express customers.

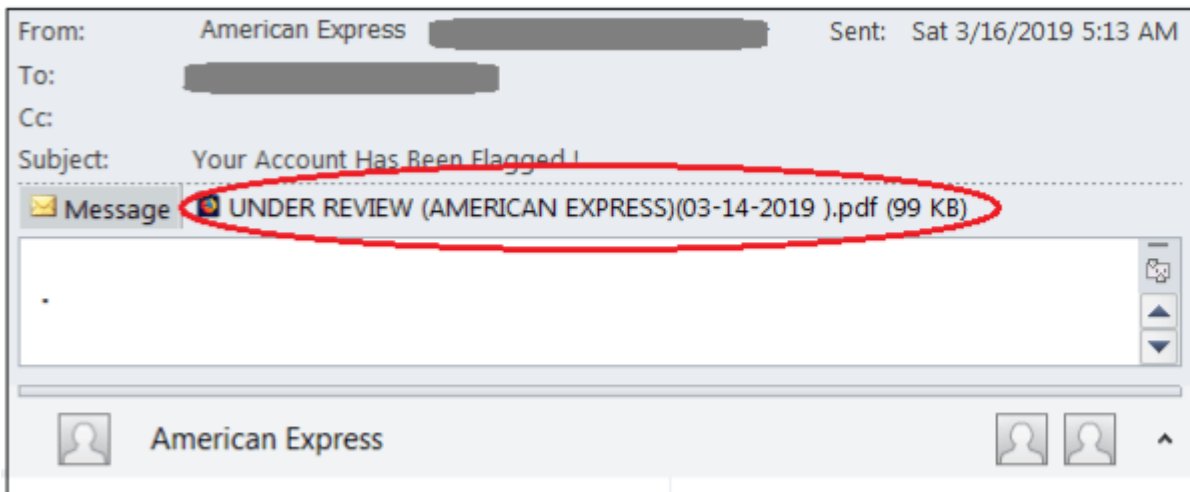


Figure 9.

“One of the highest spikes in the graph that used PDF is a phishing campaign targeting American Express during March,” researchers said.

The email purports to be from American Express, saying victims’ accounts have been flagged and featuring a PDF file that’s titled “Under Review.” When that PDF file is opened, it shows a link that leads the user to a “secure message” pretending to be from the American Express Business Card Customer Security Team. In reality the link leads the victim to a malicious landing page with a shortened URL – to further deceive victims that it’s fake – and asks for their banking credentials.

### PDF Files Used For ‘Winner Scam’

Researchers also observed a “Winner” scam, which they said was the second-highest campaign using a PDF file attachment spread via email.



Figure 10.



The attachment, claiming to be sent from Google, tells victims they won an email online sweepstake of \$1.4 million, organized by the Google Foundation and Foundation for the Promotion of Software Products.

The form then asks for personal details, and for victims to send their payment verification information via email to Google CEO Sunday Pichai at "sundarpicha@gmail[.]com."

"The scam asks the victim to provide personal details such as full name, address, country/nationality, telephone/mobile number, occupation, age/gender, and private email address," researchers said.

A message at the end of the email tell victims: "For security reasons, you are advised to keep this notification confidential as part of our precautionary measure to avoid double claims and unwarranted abuse of this program."

### **ISO and IMG Delivering AgentTesla**

Interestingly, researchers said that they've noticed a spike in attackers using disc image files (ISO and IMG files) to deliver malware since July 2018. The ISO image file is a snapshot of the data and layout of a CD; while the IMG disc image file created by various disc imaging applications.

Most notably, researchers have seen a growing number of campaigns – which albeit are smaller – using this technique to deliver AgentTesla information stealer malware and NanoCore RAT.

"Interestingly, we also have seen a recent spam campaign delivering two types of attachments: A malicious office doc and ISO image file – both installs an AgentTesla infostealer," they said.

In these campaigns, a malicious doc would execute a macro to download and execute the payload; while the ISO file would contain a malicious binary inside it.

"Regardless of which of the two attachment types the victim chooses to open, either will install AgentTesla – an infostealer that is capable of collecting the victim's system information and credentials from popular installed software such as browsers, email clients, and ftp clients," said researchers.

### **Spam Campaigns Evolving**

Spam campaigns continue to adopt new tactics that make them harder to spot – and the usage of new types of attachments, such as the ISO image file described above – only makes it easier for attackers to deceive their victims.

In fact, according to [recent research](#), spam is the most common method for cybercriminals to spread malware overall in 2018, accounting for nine out of every 10 infection attempts throughout the year.

Roughly 69 percent of spam campaigns attempted to trick users into visiting malicious URLs to download a malware-laden file or committing another online action that results in an infection.

Malicious attachments were used in the remaining 31 percent of these campaigns.

“Malware authors tend to prefer specific types of file attachments in their campaigns to distribute malicious content,” F-Secure researchers stressed.

Source: <https://threatpost.com/threatlist-top-5-most-dangerous-attachment-types/144635/>

## 5. Tales From the SOC: Hunting for Persistent Malware

At Ignite '19, Vidya Gopalakrishnan, SOC Engineer, and Matt Mellen, Sr. SOC Manager, will be giving attendees a rare glimpse into the Palo Alto Networks Security Operations Center (SOC). They'll shed light on our overall strategy as well as how [CortexXDR](#) has helped automate and enhance a tier-less security operating model. Palo Alto Networks has the benefit of being our own “customer zero” for all new Palo Alto Networks products, allowing us to make product improvements and develop best practices while keeping our security team on the cutting edge of technology. While Cortex XDR adds intelligence and efficiency into all three key functions of security operations – alert triage, incident investigation/response, and threat hunting – Vidya and Matt will be focusing specifically on how they have been using it for threat hunting, the area in which companies usually have the fewest available resources.

Here's an exclusive preview of how we've used Cortex XDR to hunt, identify, and remediate a piece of persistent malware.

### How to hunt for persistent malware

The Mitre Att&ck framework describes “persistence” as an action or config change that allows an adversary to maintain access to a system despite restarts, credential loss, or other interruptions. There are many techniques by which malware can achieve persistence; one common tactic is to change registry “run” keys, which causes a program to be executed every time a user logs in. Sounds relatively simple to identify, right? But capturing the different techniques without getting tripped up by false positives is not an easy feat without the right tools and processes.

#### Step 1: Search

Cortex XDR comes pre-configured with an array of known behavior-based indicators of compromise (BIOCs). These BIOCs are rules that identify interesting or malicious behaviors based on tactics, techniques and procedures – rather than the easily evaded artifacts typically used in IOC hunting. The first step is to search for alerts with the category of “Persistence,” and set the alert source as “[BIOCs](#).” In this case, we're targeting BIOCs that accompany typical persistence behavior, such as registry keys that have been written over or added to the registry by an unsigned process.

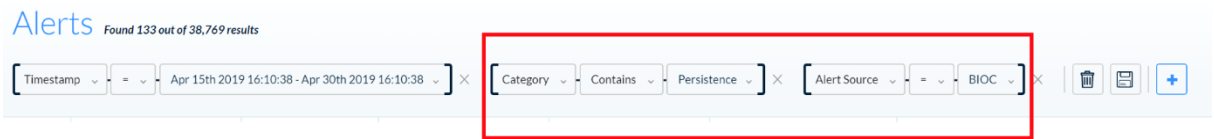


Figure 11.

### Step 2: Find what stands out

The search generates a list of events. Duplicate results from a large number of hosts generally indicates normal behavior; they can be removed. Several, however, show an executable from a suspicious path. C:/Google is definitely not a normal folder path, and the filename (oMO.exe) is also unusual.

USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY	INITIATOR CMD	ALERT NAME	DESCRIPTION
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind
PALDALTNETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup related registry keys by unsigned process	Registry   action type = registry key create, registry key rename, registry value set AND key name = 'software\Microsoft\Wind

Figure 12.

### Step 3: Triage and Validate

Selecting any one of these events, we click “Analyze” to see the chain of events (or causality). We can see that Cortex XDR identifies the root cause as cmd.exe from which everything was spawned. In the below screenshot, oMO.exe is identified as malware, which is why it shows up in red. If needed, additional information can be obtained from knowledge bases such as AutoFocus and VirusTotal with a simple right-click. The number of BIOC alerts (16) indicates that this event requires further investigation using the EDR events collected for omO.exe and the rest of the causality.



Figure 13.

### Step 4: Investigate

For further investigation, we have the option to click into several tabs revealing the forensic detail used to confirm that this is indeed malware. In these tabs, we find evidence across various types of endpoint behaviors. In the Alerts Tab, we find that the Persistence BIOC fired for the same machine 16 times. Furthermore, we can investigate the associated endpoint and network behaviors from the other tabs.

Timestamp	Host	User Name	Severity	Alert Source	Action	Category	Initiator CMD	Alert Name
Apr 25th 2019 10:07:39		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 11:07:51		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 11:07:51		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 12:08:00		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 13:08:13		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 14:13:33		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 15:19:06		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 15:19:06		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 16:19:35		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 16:19:35		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 17:20:04		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 18:20:28		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 19:20:53		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 20:21:23		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 21:16:49		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process
Apr 25th 2019 22:07:13		PALOALTONETWORK	Low	BIOC	Detected	Persistence	C:\Google\omO.EXE	New entry added to startup-related registry keys by unsigned process

Figure 14.

Looking through these tabs, we find:

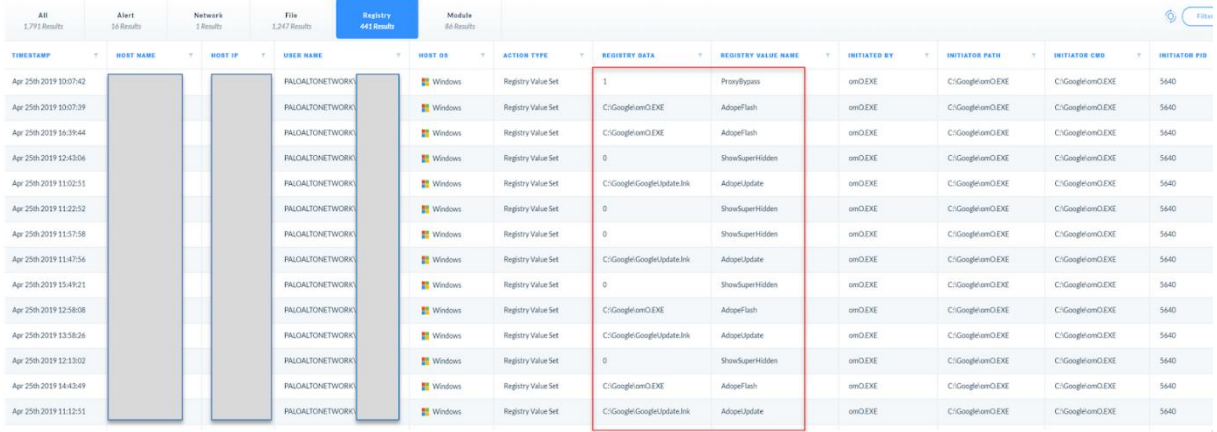
1. Registry tampering visible on the registry tab.



2. A suspicious connection to a random GoDaddy site visible on the Network tab.

3. Repetitive file reads that show the malware reading itself from the startup menu on the File tab.

Each of these is typical of persistence behavior.



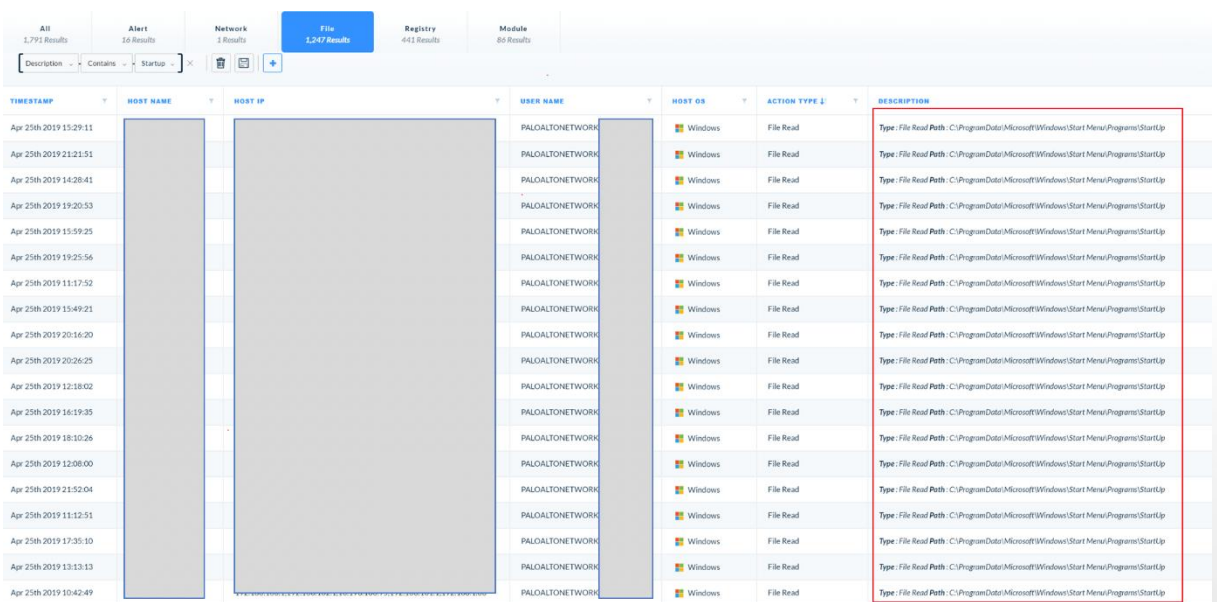
TIMESTAMP	HOST NAME	HOST IP	USER NAME	HOST OS	ACTION TYPE	REGISTRY DATA	REGISTRY VALUE NAME	INITIATED BY	INITIATOR PATH	INITIATOR CMD	INITIATOR PID
Apr 25th 2019 10:07:42			PALDALTONETWORK	Windows	Registry Value Set	1	PronyBypass	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 10:07:39			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\omO.EXE	AdopteFlash	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 16:39:44			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\omO.EXE	AdopteFlash	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 12:43:06			PALDALTONETWORK	Windows	Registry Value Set	0	ShowSuperHidden	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 11:02:31			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\GoogleUpdate.Ink	AdopteUpdate	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 11:22:52			PALDALTONETWORK	Windows	Registry Value Set	0	ShowSuperHidden	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 11:57:58			PALDALTONETWORK	Windows	Registry Value Set	0	ShowSuperHidden	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 11:47:56			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\GoogleUpdate.Ink	AdopteUpdate	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 15:49:21			PALDALTONETWORK	Windows	Registry Value Set	0	ShowSuperHidden	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 12:58:08			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\omO.EXE	AdopteFlash	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 13:56:26			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\GoogleUpdate.Ink	AdopteUpdate	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 12:13:02			PALDALTONETWORK	Windows	Registry Value Set	0	ShowSuperHidden	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 14:43:49			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\omO.EXE	AdopteFlash	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640
Apr 25th 2019 11:12:51			PALDALTONETWORK	Windows	Registry Value Set	C:\Google\GoogleUpdate.Ink	AdopteUpdate	omO.EXE	C:\Google\omO.EXE	C:\Google\omO.EXE	5640

Figure 15.



TIMESTAMP	HOST NAME	HOST IP	HOST OS	ACTION TYPE	DESCRIPTION	LOCAL IP	LOCAL PORT	REMOTE IP
Apr 25th 2019 10:07:42			Windows	Network Outgoing	Type: Network Outgoing Source	178.237.33.50:80 (www.google.com)	49548	178.237.33.50

Figure 16.



TIMESTAMP	HOST NAME	HOST IP	USER NAME	HOST OS	ACTION TYPE	DESCRIPTION
Apr 25th 2019 15:29:11			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 21:21:51			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 14:28:41			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 19:20:53			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 15:59:25			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 19:25:56			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 11:17:52			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 15:49:21			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 20:16:20			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 20:26:25			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 12:18:02			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 16:19:35			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 18:10:26			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 12:08:00			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 21:52:04			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 11:12:51			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 17:35:10			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 13:13:13			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Apr 25th 2019 10:42:49			PALDALTONETWORK	Windows	File Read	Type: File Read Path: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Figure 17.

If you're not a forensic specialist, this information can be a lot to take in, but Cortex XDR simplifies the known bad activity into contextual alerts so less experienced analysts can also perform fast and accurate investigations. This kind of information not only further confirms that this is malware but can also provide visibility into how much of our infrastructure this piece of malware may have infiltrated, to help assess the scope of damage.

### **Step 5: Remediate**

Now that we're clear that this is malicious activity, we take action. We first issue a reimage of the system given that it was affected by malware. We then blacklist the malware, preventing execution on endpoints, and do the same for the "bad domain," blocking transmission through network and cloud protection points. This, in turn, updates Wildfire where the malicious entities will be confirmed. The prevention signatures will automatically be updated on Traps and pushed to all of our global customers, thereby enabling future prevention of a malware sample that the environment has not previously seen.

### **Step 6: Breathe**

That's it – the world is now a slightly safer place.

Within a few clicks, Cortex XDR has simplified a legacy threat hunting process that is so cumbersome that companies often can't get to it, which contributes to industry statistics such as a mean-time-to-identify of 197 days.

Persistent malware is one example of structured data hunting, which is performed based on predefined behaviors that generate alerts. At Ignite, Vidya and Matt will also be sharing use cases of Cortex XDR for unstructured data hunting, using robust machine learning capabilities to find anomalies across hundreds of data dimensions. These are the types of threats that are even harder to identify using legacy approaches.

*Source:* <https://blog.paloaltonetworks.com/2019/05/xdr-tales-from-the-soc-hunting-for-persistent-malware/>

## **6. Two More Windows 10 Zero-Day PoC Exploits Released, Brings Total to 4**

After releasing exploit code for three zero-day vulnerabilities in Windows 10 over the past 48 hours, security researcher and exploit developer SandboxEscaper today has published two more, bypass for the CVE-2019-0841 patch and LPE PoC exploit dubbed InstallerBypass.

Two days ago, SandboxEscaper [released another PoC exploit for a local privilege escalation flaw](#) present in the Windows 10 Task Scheduler, leading to privilege escalation and enabling users to gain full control over files that would otherwise only be accessible by privileged users such as SYSTEM and TrustedInstaller.

Yesterday, SandboxEscaper dropped [two more PoC exploits for vulnerabilities](#) — a sandbox escape flaw present in Internet Explorer 11 (zero-day) and a local privilege escalation vulnerability impacting Windows Error Reporting (already patched).

The reason given for releasing these vulnerabilities like this are in a post from May 22 from SandboxEscaper's blog. Today, another post states that these two were the last remaining bugs:

*Uploaded the remaining bugs.*

*I like burning bridges. I just hate this world.*

*ps: that last windows error reporting bug was apparently patched this month. Other 4 bugs on github are still 0days. have fun.*

### **Local privilege escalation PoC**

The zero-day local privilege escalation (LPE) flaw dubbed [CVE-2019-0841-BYPASS](#) was found by SanboxEscaper after noticing that "there is still a vuln in the code triggered by CVE-2019-0841."

CVE-2019-0841 is a "Windows Elevation of Privilege Vulnerability" that [was patched](#) during the May 2019 Patch Tuesday updates.

*"An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data."*

According to the researcher, this new vulnerability bypasses Microsoft's CVE-2019-0841 patch and it allows attackers to write the discretionary access control list (DACL) which "identifies the trustees that are allowed or denied access to a securable object" after successful exploitation.

As she describes the exploitation process:

*If you create the following:*

*(GetFavDirectory() gets the local appdata folder, fyi)*

```
CreateDirectory(GetFavDirectory()                                     +
L"\\Packages\\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\\Microsoft.MicrosoftEdge_44.1
7763.1.0_neutral__8wekyb3d8bbwe",NULL);
CreateNativeHardlink(GetFavDirectory()                             +
L"\\Packages\\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\\Microsoft.MicrosoftEdge_44.1
7763.1.0_neutral__8wekyb3d8bbwe\\bear3.txt",L"C:\\Windows\\win.ini");
```

*If we create that directory and put an hardlink in it, it will write the DACL.*

!!IMPORTANT!!  
Microsoft.MicrosoftEdge\_44.17763.1.0\_neutral\_\_8wekyb3d8bbwe this part has to reflect  
the currently installed edge version.  
You can find this by opening edge -> settings and scrolling down.  
!!IMPORTANT!!

SandboxEscaper provides PoC executables in the CVE-2019-0841-BYPASS' repository PoCFiles folder which can be used to test the vulnerability on patched Windows machines.

A video demo of the proof-of-concept exploit in action was also provided by the researcher on GitHub: <https://vimeo.com/338017995>

BleepingComputer compiled the PoC from source to target the current versions of Edge and was able to confirm that it would indeed allow users to gain full control over files after successful exploitation as seen in the screenshots below.

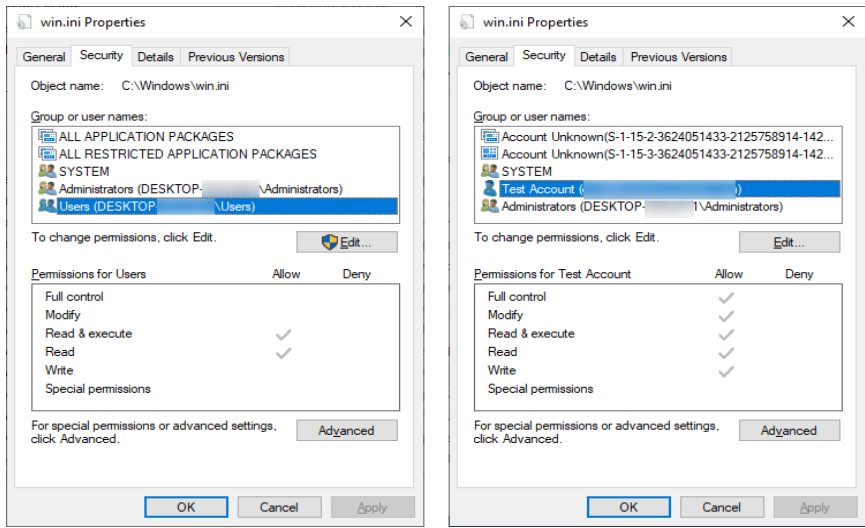


Figure 18. User permissions before and after the PoC is executed

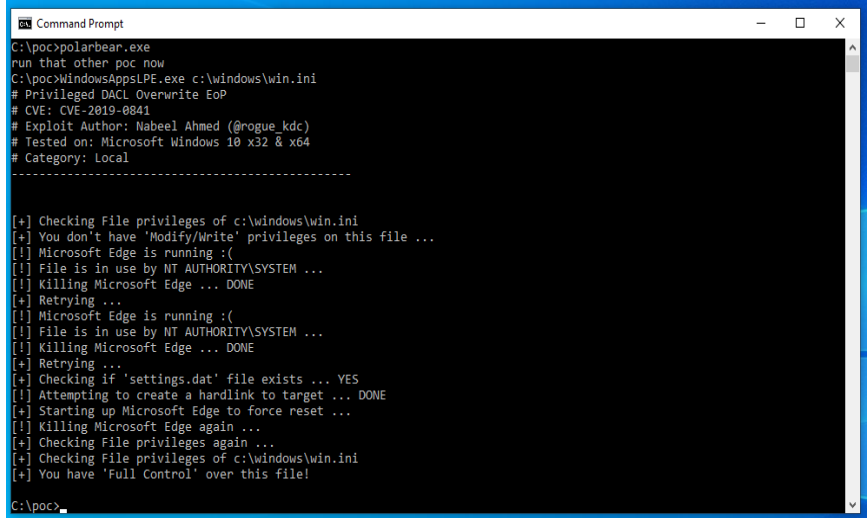


Figure 19.

### Hard to reproduce LPE PoC

The other zero-day PoC exploit released by the researcher today and dubbed InstallerBypass is also for a local privilege escalation vulnerability and it can be used to drop binaries into the system32 Windows folder and run them with escalated privileges.

As SandboxEscaper says, it "Could be used with malware, you could programmatically trigger the rollback. Maybe you can even pass the silent flag to hide installer UI and find another way to trigger rollback (i.e through installer api, injecting into medium IL msiexec etc)."

She also provides a detailed reproduction procedure which might prove to be problematic because of a "really small timing window" and a video demo of the zero-day PoC in action: <https://vimeo.com/338018548>

Source: <https://www.bleepingcomputer.com/news/security/two-more-windows-10-zero-day-poc-exploits-released-brings-total-to-4/>

## 7. Calibration Attack Drills Down on iPhone, Pixel Users

A new way of tracking mobile users creates a globally unique device fingerprint that browsers and other protections can't stop.

A proof-of-concept for a new type of privacy attack, dubbed "calibration fingerprinting," uses data from Apple iPhone sensors to construct a globally unique fingerprint for any given mobile user. Researchers said that this provides an unusually effective means to track people as they browse across the mobile web and move between apps on their phones.

Further, the approach also affects Pixel phones from Google, which run on Android.

A research team from the University of Cambridge in the UK [released their findings](#) this week, showing that data gathered from the accelerometer, gyroscope and magnetometer sensors found in the smartphones can be used to generate the calibration fingerprint in less than a second – and that it never changes, even after a factory reset.

The attack also can be launched by any website a person visits via a mobile browser, or any app, without needing explicit confirmation or consent from the target.

In Apple's case, the issue results from a weakness in iOS 12.1 and earlier, so iPhone users should update to the latest OS version as soon as possible. Google has not yet addressed the problem, according to the researchers.

### Next-Gen Device Fingerprinting

A device fingerprint allows websites to detect return visits or track users, and in its innocuous form, can be used to protect against identity theft or credit-card fraud; advertisers often also rely on this to build a user profile to serve targeted ads.



Fingerprints are usually built with pretty basic info: The name and version of your browser, screen size, fonts installed and so on. And browsers are increasingly using blocking mechanisms to thwart such efforts in the name of privacy: On Apple iOS for iPhone for instance, the Mobile Safari browser uses Intelligent Tracking Prevention to restrict the use of cookies, prevent access to unique device settings and eliminate cross-domain tracking.

However, any iOS devices with the iOS version below 12.2, including the latest iPhone XS, iPhone XS Max and iPhone XR, it's possible to get around those protections, by taking advantage of the fact that motion sensors used in modern smartphones use something called microfabrication to emulate the mechanical parts found in traditional sensor devices, according to the paper.

"MEMS sensors are usually less accurate than their optical counterparts due to various types of error," the team said. "In general, these errors can be categorized as deterministic and random. Sensor calibration is the process of identifying and removing the deterministic errors from the sensor."

Websites and apps can access the data from sensors, without any special permission from the users. In analyzing this freely accessible information, the researchers found that it was possible to infer the per-device factory calibration data which manufacturers embed into the firmware of the smartphone to compensate for these systematic manufacturing errors. That calibration data can then be used as the fingerprint, because despite perceived homogeneity, every Apple iPhone is just a little bit different – even if two devices are from the same manufacturing batch.

"We found that the gyroscope and magnetometer on iOS devices are factory-calibrated and the calibration data differs from device-to-device," the researchers said. "Extracting the calibration data typically takes less than one second and does not depend on the position or orientation of the device."

To create a globally unique calibration footprint requires adding in a little more information, however, for instance from traditional fingerprinting sources.

"We demonstrated that our approach can produce globally unique fingerprints for iOS devices from an installed app — around 67 bits of entropy for the iPhone 6S," they said. "Calibration fingerprints generated by a website are less unique (~42 bits of entropy for the iPhone 6S), but they are orthogonal to existing fingerprinting techniques and together they are likely to form a globally unique fingerprint for iOS devices."

A longitudinal study also showed that the calibration fingerprint, which the researchers dubbed "SensorID," doesn't change over time or vary with conditions.

"We have not observed any change in the SensorID of our test devices in the past half year," they wrote. "Our dataset includes devices running iOS 9/10/11/12. We have tested compass calibration, factory reset, and updating iOS (up until iOS 12.1); the SensorID always stays the

same. We have also tried measuring the sensor data at different locations and under different temperatures; we confirm that these factors do not change the SensorID either.”

### **Widely Exploitable**

In terms of how applicable the SensorID approach is, the research team found that both mainstream browsers (Safari, Chrome, Firefox and Opera) and privacy-enhanced browsers (Brave and Firefox Focus) are vulnerable to the attack, even with the fingerprinting protection mode turned on.

Further, motion sensor data is accessed by 2,653 of the Alexa top 100,000 websites, the research found, including more than 100 websites exfiltrating motion-sensor data to remote servers.

“This is troublesome since it is likely that the SensorID can be calculated with exfiltrated data, allowing retrospective device fingerprinting,” the researchers wrote.

However, it’s possible to mitigate the calibration fingerprint attack on the vendor side by adding uniformly distributed random noise to the sensor outputs before calibration is applied at the factory level – something Apple did starting with iOS 12.2.

“Alternatively, vendors could round the sensor outputs to the nearest multiple of the nominal gain,” the paper said.

Privacy-focused mobile browsers meanwhile can add an option to disable the access to motion sensors via JavaScript.

“This could help protect Android devices and iOS devices that no longer receive updates from Apple,” according to the paper.

### **Google Pixel Devices**

Although most of the research focused on iPhone, Apple is not the only vendor affected: The team found that the accelerometer of Google Pixel 2 and Pixel 3 can also be fingerprinted by the approach.

That said, the fingerprint has less individual entropy and is unlikely to be globally unique – meaning other kinds of fingerprinting data would also need to be gathered for full device-specific tracking.

Also, the paper noted that other Android devices that are also factory calibrated might be vulnerable but were outside the scope of testing.

While Apple addressed the issue, Google, which was notified in December about the attack vector, is still in the process of “investigating this issue,” according to the paper.

Source: <https://threatpost.com/calibration-attack-iphone-pixel/145037/>

## 8. Android Users Being Spammed Using Fake Missed Call Alerts

Scammers are abusing the Notifications and Push APIs and Google Chrome on Android devices to push spam alerts customized to look like a missed phone call.

The two APIs are used on mobile devices for push notifications - short alerts designed to re-engage the user. The messages can be triggered by a local application or a server, regardless if the app is running or not.

"The Notifications API lets us display notifications to the user. It is incredibly powerful and simple to use. Where possible, it uses the same mechanisms a native app would use, giving a completely native look and feel," reads the description for the Notifications API.

### Fraudsters change Chrome's icon

Lookout's Phishing AI service caught a phishing campaign that is currently pushing messages to mobile users with a custom icon for the application that triggers the alert, which in this case is Google Chrome.

To disguise the origin, the scammers changed the browser's icon to read "Missed call" as if it is a missed call notification. One message announces that the user has an iPhone XS waiting for them; another simply informs of an alleged missed call from Esmeralda, the medium.

This is powerful social engineering as users frequently rely on visual indicators to identify the origin of an alert.

"Scammers are looking to take advantage of the fact that we're primed to identify certain icons we normally associate with system messages (in this case the icon of the telephone)," Jeremy Richards, security researcher at Lookout, told BleepingComputer.

It is important to note that the message is not displayed unless the victim decides to accept notifications from the spammy domain. This means that sites that earned the trust of the user can be used for this type of phishing campaigns.

Below is a short list of domains that serve spam via push notifications on mobile devices:

*Consumertestconnect[.]com*

*foundmoneyguide[.]com*

*getitfree-samples[.]com*

*click4riches[.]info*

*yousweeps[.]com (this domain hosts tens of spam templates for various brands)*

Not all notification spam uses the trick of changing the browser's icon, but they have messages that are sufficiently alluring to claim a few victims.

### Same approach possible on desktops

Richards saw this activity on Android mobile phones and the reason for this is that push notifications for Safari on iOS are not fully supported at the moment; but the same approach

is suitable for desktop, too. Safari and Chrome support web-based notifications and can be used to spawn a fake card.

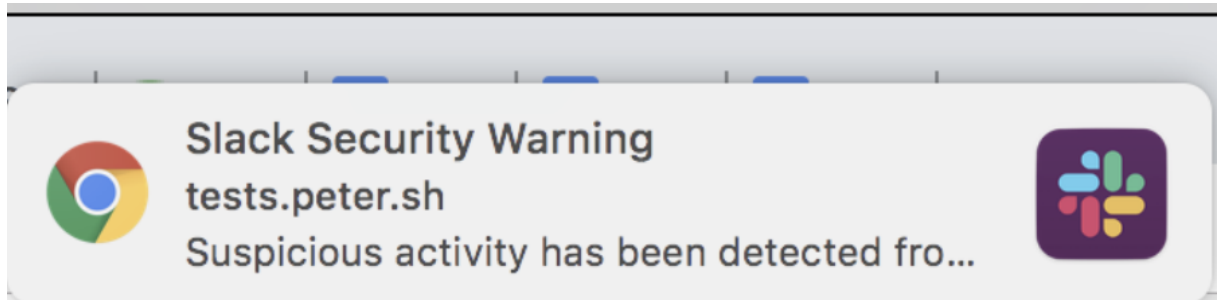


Figure 20. Credit: Jeremy Richards

A quick read of the text and looking at the Slack icon could easily fool a user into clicking the alert and landing on a phishing page that captures credentials.

On mobile, the same alert is even more credible, as the only giveaways would be Chrome's name, the app that triggers the notification, and the domain pushing the spam. When Chrome's icon is changed, there is little to hint at the forged nature of the message, as only the name of the browser and the domain indicate the fraud attempt.

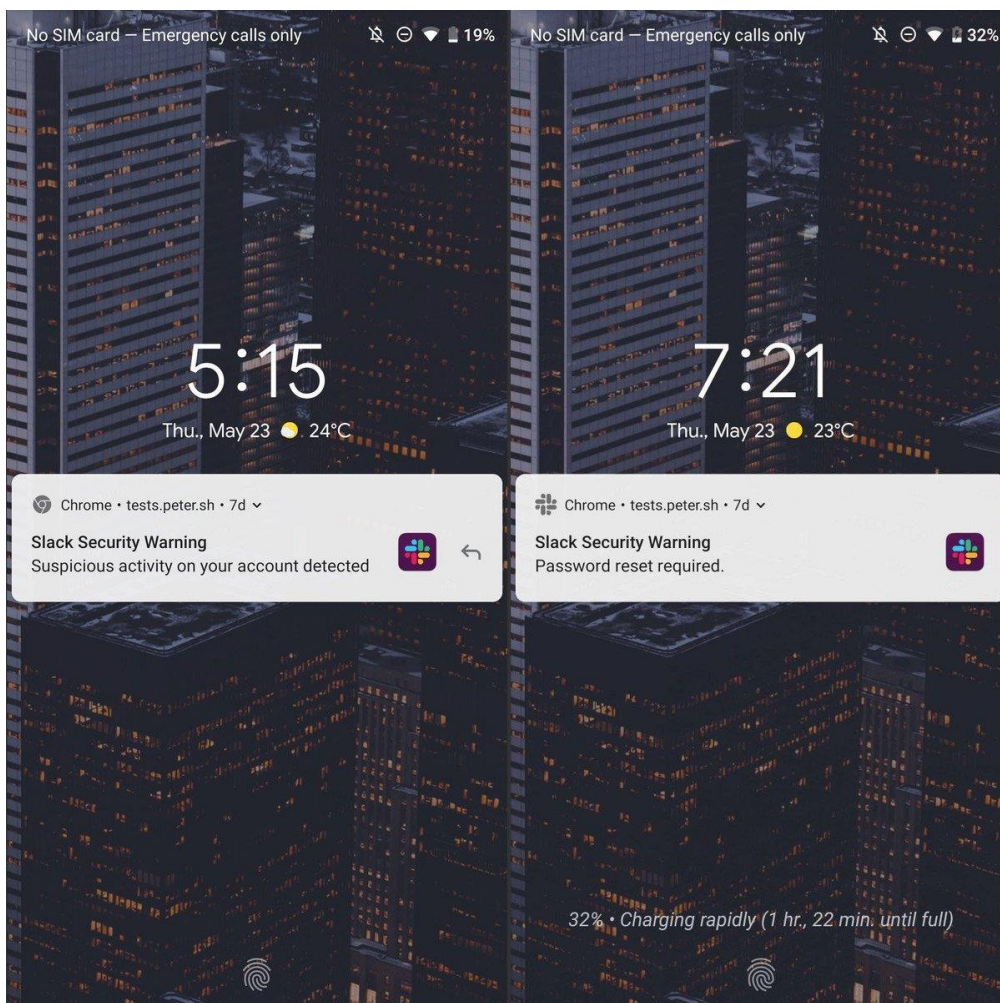


Figure 21.

Google software engineer Peter Beverloo created a notification generator that can be used to test how a push card appears on both desktop and mobile devices.

The tool allows typing a custom title and body for the message as well as add an assortment of pictures (icon, badge, image) and actions.

Source: <https://www.bleepingcomputer.com/news/security/android-users-being-spammed-using-fake-missed-call-alerts/>

## 9. Snapchat Privacy Blunder Piques Concerns About Insider Threats

After a report found that Snap employees were abusing their access to Snapchat data, experts are warning that insider threats will continue to be a top challenge for privacy.

Snap, the company behind the popular Snapchat social media app, has found itself in hot water after a recent report revealed that Snap employees were abusing their access to private user data – which includes location data, saved Snaps and phone numbers.

According to a Thursday Motherboard report, Snap touted several internal tools enabling employees to access Snapchat users' personal data. One such tool, dubbed SnapLion, was originally created to help collect data in response to law enforcement requests via court orders. However, several internal emails obtained by Motherboard showed several employees abused this capability, with one Snap employee looking up an email address for an account outside of a law enforcement situation, for instance.

The report raises several important questions about data privacy. While it may be inevitable that employees of companies have access to floods of data, companies face a serious challenge in preventing their own employees from abusing these privileges.

"As organizations grow, especially if they grow very quickly, it can be challenging to manage controls around customer privacy," Tim Erlin, VP of product management and strategy at Tripwire, told Threatpost. "Consumers suffer from a lack of transparency in how their personal data is handled, managed and viewed after it leaves their proverbial hands. There is simply no way for me, as a consumer, to know who has access to my data once a company takes possession of it, and that fact leaves room for abuse to occur."

This recent incident with Snap in particular raises concerns because of just how personal the data being collected is. That data includes saved Snaps themselves – photos or videos sent between Snapchat users that disappear after opened (but which can also be "saved" by the sender), location data, email addresses and phone numbers tied to accounts.

Specifically, the report raises questions about what types of restrictions Snap places on employee access to data and how it keeps track of that access. Snap for its part told Motherboard that it monitors all access to data, and limits access to the internal tools like



SnapLion to only those who need it. According to the report, Snap does have a logging system that enables the company to track who uses systems and which data is accessed – but anonymous former employees told Motherboard that the logging isn't perfect.

George Wrenn, CEO of CyberSaint Security, told Threatpost organizations like Snap with widespread data access must be extremely careful when standardizing, measuring, and especially communicating the depth and breadth of their privacy and data protection programs.

"Clear communication and management from the board level down to every employee is key to the success and scalability of companies such as these," he said. "Moving forward, it will be necessary for success as systems become more complex, and as personal data protection and privacy continue to shift to the forefront of our country's concern."

Insider threats continue to be a top concern across the industry. In fact, according to the Verizon Data Breach Investigations Report from this year, "privilege misuse and error by insiders" account for 30 percent of breaches.

And it's not just Snap – a report last year found that Facebook had fired an employee who allegedly abused their access to data to stalk women.

Willy Leichter, vice president of marketing at Virsec, told Threatpost, that arguably, too much cyber privacy discussion is around egregious breaches or external leaks of private data rather than internal employee incidents.

"While [external leaks] are newsworthy, the broader question is how much trust we put in online services to whom we've voluntarily given information," said Leichter. "Privacy regulations like the GDPR do have requirements for minimizing use of personal data to specific authorized activities, but oversight and enforcement of internal abuse rarely exists. The temptation for abuse is just too great for online services that monetize data to find creative ways to go over the line."

Snap, for its part, didn't respond to a request for comment from Threatpost.

Source: <https://threatpost.com/snapchat-privacy-blunder-piques-concerns-about-insider-threats/145074/>

## 10. macOS Unpatched for Executing Untrusted Code off the Network

### Abusing legitimate features

According to details from Filippo Cavallarin of cyber security company Segment in Italy, Gatekeeper treating external drives and networks as safe locations can be combined with other legitimate features on macOS to execute untrusted apps without warning the user.

Using the automount functionality in Apple's OS and the support for symbolic links, it is possible to run arbitrary code without triggering a reaction from Gatekeeper. On macOS, a user can automatically mount network shares using the 'autofs' command.

Symbolic links are files that create a reference to other files or folders stored in a different location, including a network share. They are not verified when present in archives, so users can be tricked to click them and access content stored in a remote location.

Cavallarin's method is simple. In his proof-of-concept, he modified the files of the Calculator app to include a bash script that launches a different executable, in this case iTunes; he also changed the Calculator app's icon. He shows in a video demo that this can be used to obtain a reverse shell on the target computer.

The Gatekeeper bypass technique is present in [MITRE's catalog](#) of adversary tactics and techniques:

*In macOS and OS X, when applications or programs are downloaded from the internet, there is a special attribute set on the file called com[.]apple[.]quarantine. This attribute is read by Apple's Gatekeeper defense program at execution time and provides a prompt to the user to allow or deny execution.*

*Apps loaded onto the system from USB flash drive, optical disk, external hard drive, or even from a drive shared over the local network won't set this flag. Additionally, other utilities or events like drive-by downloads don't necessarily set it either. This completely bypasses the built-in Gatekeeper check.*

The researcher published the complete details for the attack and a video demonstrating the validity of his findings: <https://www.youtube.com/watch?v=m74cpadIPZY>

*To better understand how this exploit works, let's consider the following scenario:*

- 1. An attacker crafts a zip file containing a symbolic link to an automount endpoint she/he controls (ex Documents -> /net/evil.com/Documents) and sends it to the victim.*
- 2. The victim downloads the malicious archive, extracts it and follows the symlink*

In this context, the victim accesses code from a location that is controlled by the attacker and trusted implicitly by Gatekeeper. Executing an app this way does not trigger the security mechanism in macOS.

The attack is valid and was replicated by Sabina Alexandra Ștefănescu, security professional and co-founder of Security Espresso, a community at the intersection of programming and security. Using the same technique, she was able to add to the Calculator app a script that launched iTunes. Her test system was running macOS Mojave 10.14.5.

Cavallarin says that because Finder is designed to hide app extensions and the full path from the title bar, users would have a hard time spotting the attack. However, a hacker would first need access to the network to pull off this attack, which may not go undetected.

A potential solution for this issue is to disable automatic mounting of network shares by following the steps below:

1. *Edit /etc/auto\_master as root*
2. *Comment the line beginning with '/net'*
3. *Reboot*

Cavallarin claims he informed Apple of the issue on February 22 and that the company should have fixed it with the security updates in May. The researcher says that the issue is still there and that "Apple started dropping my emails."

"Since Apple is aware of my 90 days disclosure deadline, I make this information public," the researcher says.

The researcher told BleepingComputer that he had tested the attack on Mojave 10.14.5 a few hours before publishing the details on Friday.

In this month's security updates for macOS, Apple released a patch for an issue - tracked as CVE-2019-8589, that allowed a malicious application to bypass Gatekeeper. The fix is available for macOS Mojave 10.14.4, though, and is a different bug than what Cavallarin reported.

Source: <https://www.bleepingcomputer.com/news/security/new-unpatched-macos-gatekeeper-bypass-published-online/>

## 11. Malspam Campaigns Use HawkEye Keylogger to Target Businesses

Attackers have been observed targeting businesses on a worldwide scale during the last two months with the HawkEye keylogger malware according to a report from IBM X-Force.

As part of the April and May malicious campaigns which focused on business users, attackers used malspam emails to target organizations from numerous industry sectors like "transportation and logistics, healthcare, import and export, marketing, agriculture, and others."

"HawkEye is designed to steal information from infected devices, but it can also be used as a loader, leveraging its botnets to fetch other malware into the device as a service for third-party cybercrime actors," says IBM X-Force's research team.

### April and May HawkEye campaigns

The malspam campaigns which disseminate the keylogger are actively targeting business users in an effort to steal both accounts credentials and sensitive data that could be later put to use as part of account takeover or business email compromise attacks.

During the April and May Hawkeye campaigns, attackers using spam servers located in Estonia disguised the malicious spam emails as messages from Spanish banks or legitimate companies, distributing both HawkEye Reborn v8.0 and HawkEye Reborn v9.0.

While the spam emails used generic greetings, featured poor quality text and content, and did not feature any company logos, "the spammers managed to spoof the sending address to appear to originate from a large bank's domain."

The malspam emails come with attachments containing fake commercial invoice which, once opened by the victim, will drop the HawkEye malware in the background while displaying the commercial invoice image as a distraction.

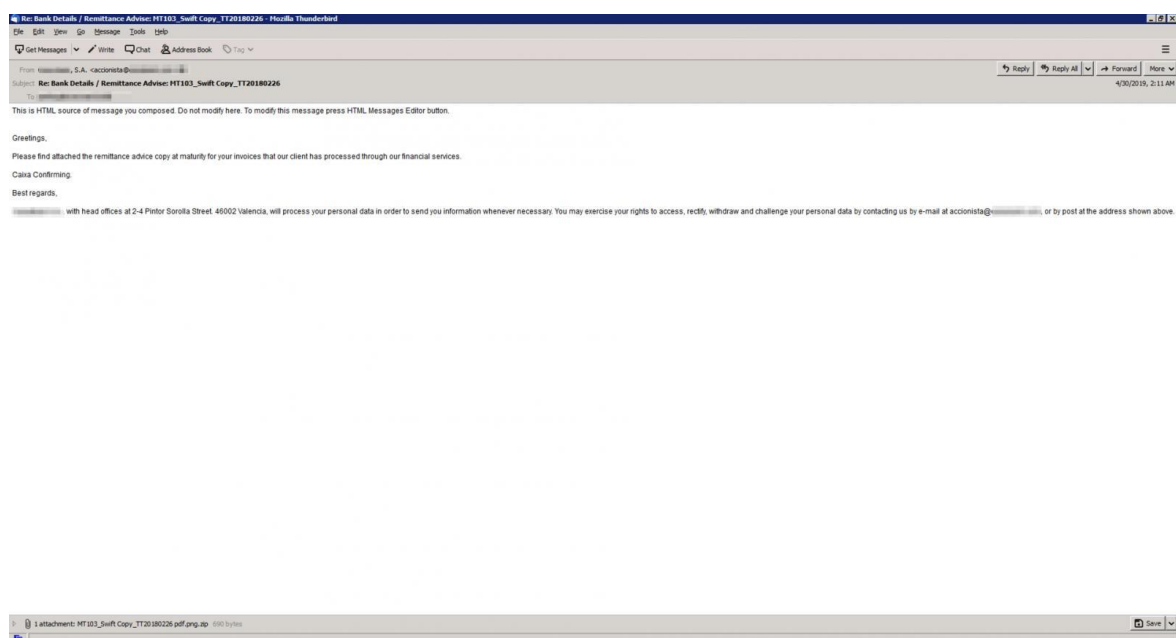


Figure 22. Sample malspam email

"Samples we checked reached users in Spain, the US, and the United Arab Emirates for HawkEye Reborn v9. HawkEye v8 focused on targeting users in Spain," says IBM X-Force's analysis.

To infect the victims with the keylogger/stealer malware, a mshta.exe binary dropped by PhotoViewer when the victim tries to open the fake invoice will use PowerShell to connect to the command-and-control (C2) server and drop additional malware payloads.

The malware gains persistence on the compromised system with the help of an AutoIt script in the form of an executable named gvg.exe which adds itself as an AutoRun entry to the Windows Registry, thus making sure that it will get relaunched automatically after each system restart.

The IBM X-Force researchers also discovered that "the second line in the script shows a file named AAHEP.txt. That file contains all the necessary instructions concerning the functions and commands related to the actual Hawkeye Keylogger."

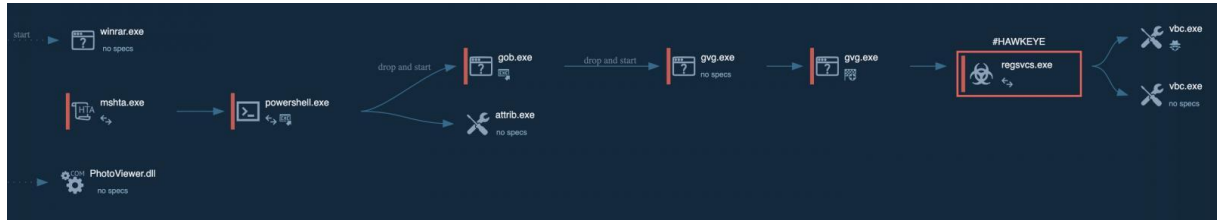


Figure 23. Infection process

### HawkEye-powered malspam campaigns

When looking into the list indicators of compromise for the April and May 2019, the X-Force researchers found another malspam campaign launched from a server from Turkey "between February 11, 2019 and March 3, 2019" but with an IP address from the same class C network.

Coupled with the fact that both campaigns feature very similar attack patterns with emails dropping malware payloads disguised as commercial invoices which would infect the targets with an info-stealing Trojan, led the X-Force researchers to think that they are operated by the same threat actor.

Other malspam campaigns disseminating the Hawkeye keylogger were also detected by Cisco Talos during April, as well as My Online Security during May, with the latter noticed that the data was either exfiltrated to the servers of another keylogger named Spytector or that the attackers were using a compromised Spytector email to collect the stolen data.



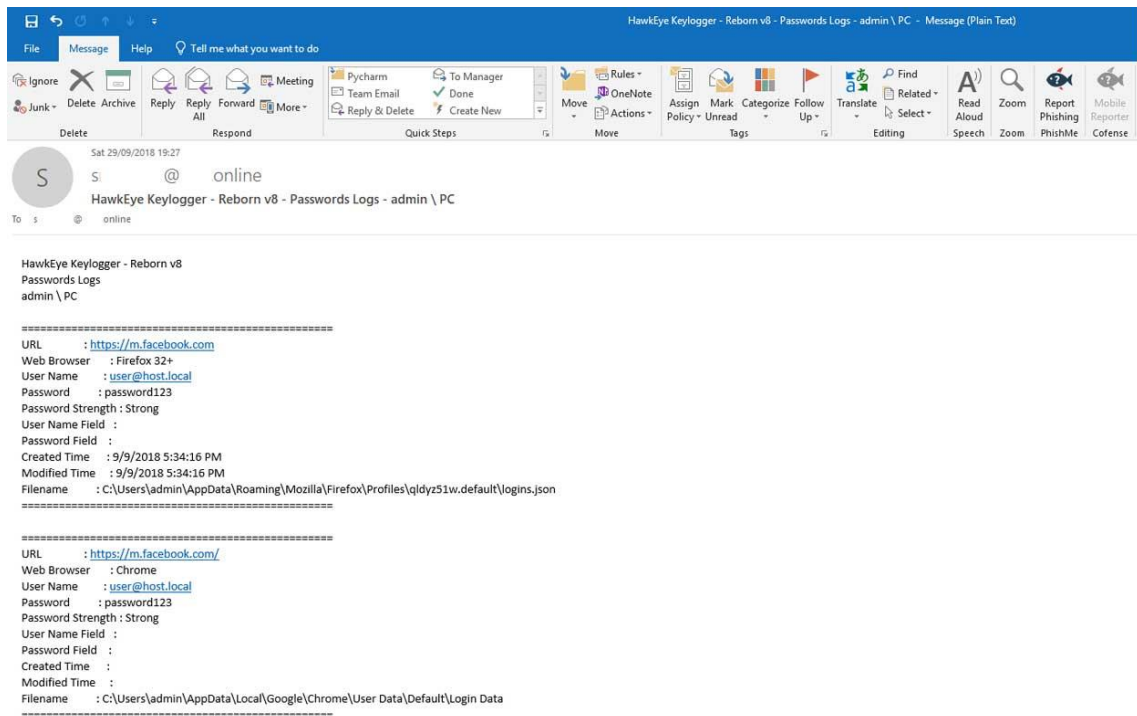


Figure 24. Email sent by the Hawkeye Keylogger to its operators (Image: Cofense)

## The HawkEye Reborn v9 malware kit

The HawkEye keylogger and information stealer malware kit has been in development since about 2013, with a multitude of new features and modules added by its developers throughout the years to boost its monitoring and data theft capabilities.

Hawkeye is being sold by its development team on dark web markets and hacking forums, and it is currently being distributed through resellers after it has changed owners in December 2018.

HawkEye Reborn v9, the latest version of the malware kit, can collect information from various applications which it then ships to its operators via protocols such as FTP, HTTP, and SMTP.

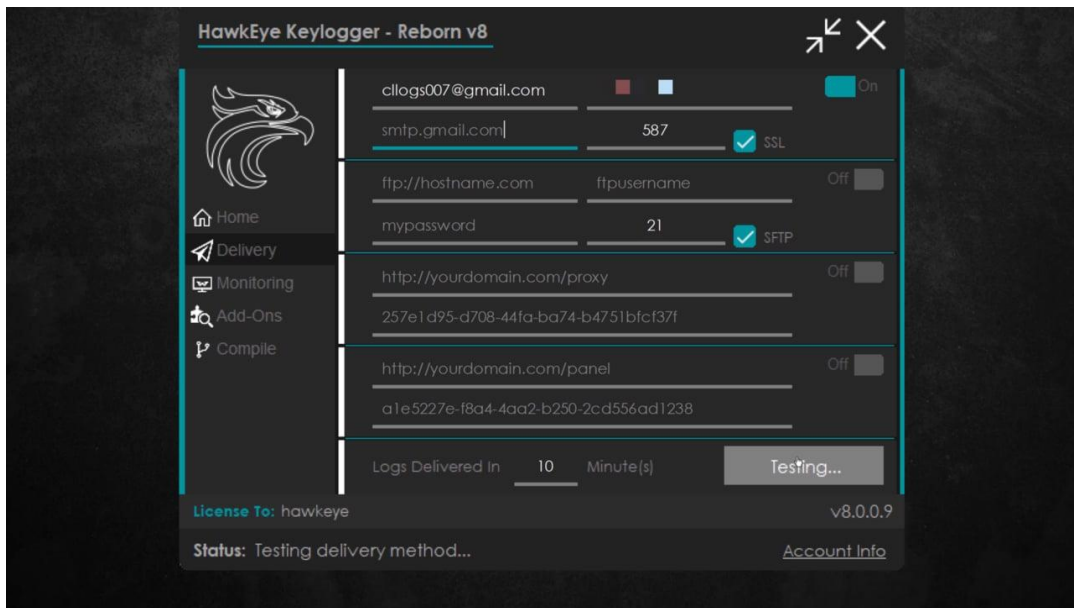


Figure 25. HawkEye Reborn UI

"Recent changes in both the ownership and development efforts of the HawkEye Reborn keylogger/stealer demonstrate that this is a threat that will continue to experience ongoing development and improvement moving forward," said Cisco Talos' research team in its analysis of the HawkEye Reborn v9 keylogger/stealer malware.

"HawkEye has been active across the threat landscape for a long time and will likely continue to be leveraged in the future as long as the developer of this kit can monetize their efforts."

Source: <https://www.bleepingcomputer.com/news/security/malspam-campaigns-use-hawkeye-keylogger-to-target-businesses/>

*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](mailto:asoc.sales@telelink.com)

**Advanced Security Operations Center**

**Telelink Business Services**

[www.telelink.com](http://www.telelink.com)