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

Monthly Security Bulletin

August 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					
⬛ 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 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

Contents

Executive summary 4
1. An entire nation just got hacked 6
Hackers' paradise 6
'Very embarrassing for the government' 7
2. Dating App Jack'd Fined After Leaking Users' Nude Pics 8
3. Billions of Records Including Passwords Leaked by Smart Home Vendor 10
Securing ElasticSearch servers 12
4. Mac Malware Pushed via Google Search Results, Masking as Flash Installer 13
5. BianLian Android Banking Trojan Upgraded With Screen Recorder 15
6. New Backdoor and Malware Downloader Used in TA505 Spam Campaigns 18
Ongoing TA505 campaigns 20
Ransomware, Trojans, and RATs on the menu 21
7. PGP Ecosystem Targeted in 'Poisoning' Attacks 22
8. Microsoft Discovers Fileless Astaroth Trojan Campaign 23
9. GoBotKR Targets Pirate Torrents to Build a DDoS Botnet 26
10. Dridex Banking Trojan, RMS RAT Dropped via Fake eFax Messages 27
Web injects used to abuse victims' web browsers 28
Several types of sites targeted using multiple injects 29
11. Rig Exploit Kit Pushing Eris Ransomware in Drive-by Downloads 30
The ERIS Ransomware 31
12. New eCh0raix Ransomware Brute-Forces QNAP NAS Devices 32
Encrypting victim's files 33
Decryptor not available yet 37
13. Cisco ASA and FTD Software TLS and SSL Driver DoS Vulnerability 37
14. Hacked Hair Straighteners Can Threaten Homes 38
15. New DoppelPaymer Ransomware Emerges from BitPaymer's Code 39
Victims in the public service sector 39
Parallel extortion activity 40
16. Turla APT Returns with New Malware, Anti-Censorship Angle 42
Latest Toolset 42
17. BEC Scams Average $301 Million Per Month In Illegal Transfers 43
Statistics are dire 44
Most common victims 45
Top BEC methods 46
18. Facebook to Pay Over $5 Billion Following FTC, SEC Settlements 47
$100 million SEC settlement 49

Executive summary

1. Financial records, names, ID numbers, e-mail addresses and passwords for 5 milion citizens were leaked from hacker that breached Bulgarian National Revenue Agency. Police arrested one suspect already and charged his employer – an Bulgarian cyber-security company with cyber terrorism. →
2. LGBQT dating app Jack'd has been slapped with a $240,000 fine after data breach that leaked personal data and nude photos of its users. The exposed information could potentially put users at risk of arrest in certain countries and the company seems to have been notified back in February from independent researcher →
3. A publicly accessible ElasticSearch cluster owned by Orvibo, a Chinese smart home solutions provider, leaked more than two billion user logs containing sensitive data of customers from China, Japan, Thailand, the US, the UK, Mexico, France, Australia, and Brazil. →
4. Never-before-seen Mac malware, named OSX/CrescentCore, has been discovered masquerading as an Adobe Flash Player installer. The malware was also spread via high-ranking Google search results. →
5. Known BianLian banking Trojan has been upgraded by his authors with two new modules able to record the screens of infected Android devices and to create a SSH server for camouflaging its communication channels. The extra components allow the malware to send text messages, to run arbitrary USSD codes, lock the screens of compromised devices, inject push notifications and perform overlay attacks. →
6. TA505 hacking group that was behind the Dridex banking trojan and Locky ransomware is running several new malicious spam campaigns to spread new malware strains with the Gelup downloader and the FlowerPippi backdoor in the Middle East, Japan, India, the Philippines, and Argentina. The spam emails contain .DOC and .XLS documents to disseminate its new malware, with the payloads being dropped on compromised machines via VBA macros. →
7. Unknown adversaries have singled out two recognized experts in the field of OpenPGP email encryption and are executing attack, called certificate spamming, that misuses keyserver verification directories and makes it impossible for Pretty Good Privacy (PGP) to work properly for those targeted. →
8. A fileless malware campaign using information stealing Astaroth Trojan injected into the memory of infected computers was detected by Microsoft Defender ATP Research Team. The malware strain is capable of stealing sensitive information such as user credentials from its victims using a key logger module, operating system calls interception, and clipboard monitoring. →
9. A botnet dubbed GoBotKR is targeting fans of Korean TV, compromising computers via pirated copies of South Korean movies, games and TV shows available via Korean and Chinese torrent sites. →
10. New malspam campaign is identified that delivers fake eFax messages designed to drop a malware cocktail via malicious Microsoft Word document. The phishing emails include

ZIP archived XLS Microsoft Excel documents with a macro designed to download and launch Dridex and Remote Manipulator System Remote Access Tool (RMS RAT) malicious payloads, capable of collecting credentials from web browsers, to exfiltrate them to external servers and managing the infected computers. →

11. The RIG exploit kit has been spotted distributing the new ERIS Ransomware as its payload. Using the RIG exploit kit, vulnerable victims will find that the ransomware is installed on their computer without their knowledge simply by visiting a web site. →
12. New ransomware strain written in Go and dubbed eCh0raix by the Anomali Threat Research Team is being used in the wild to infect and encrypt documents on consumer and enterprise QNAP NAS devices. Devices are being attacked through weak credentials and by exploiting known vulnerabilities, however the malware skips targets, located in Belarus, Ukraine, or Russia.→
13. A vulnerability in the cryptographic driver for Cisco Adaptive Security Appliance Software (ASA) and Firepower Threat Defense (FTD) Software due to incomplete input validation of a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) ingress packet header could allow an unauthenticated, remote attacker to cause the device to reboot unexpectedly. →
14. Researchers have found a way to successfully hack Glamoriser hair straightener via Bluetooth Low Energy (BLE) embedded for connecting to a mobile app to turn them on and increase the heating element up to its maximum temperature—causing a serious fire hazard for unsuspecting owners. →
15. New file-encrypting malware dubbed DoppelPaymer that has been making victims since at least mid-June is asking hundreds of thousands of US dollars in ransom. The ransomware strain has at least eight variants that extended their feature set gradually, with the earliest one dating since April. Victims in the public service sector DoppelPaymer takes its name from BitPaymer, with which it shares more than large portions of code. →
16. Turla APT has revamped its arsenal in 2019, creating new weapons and tools for targeting government entities. It's now using booby-trapped anti-internet censorship software as an initial infection vector with C2 infrastructure hosted on compromised WordPress sites and on cloud services. →
17. The frequency of business email compromise (BEC) scams has increased year over year and so did the value of attempted thefts, reaching a monthly average of more than $300 million and increase from 500 in 2016 to more than 1,100 in 2018. Companies lost $1.2 billion to this sort of cybercriminal activity →
18. An agreement with the FTC requires Facebook to pay largest ever consumer privacy violation penalty of $5 billion, to implement a new privacy and information protection framework, and to provide new monitoring tools after an investigation launched following the Cambridge Analytica events. →

1. An entire nation just got hacked

(CNN) - Asen Genov is pretty furious. His personal data was made public this week after records of more than 5 million Bulgarians got stolen by hackers from the country's tax revenue office.

In a country of just 7 million people, the scale of the hack means that just about every working adult has been affected.

"We should all be angry. ... The information is now freely available to anyone. Many, many people in Bulgaria already have this file, and I believe that it's not only in Bulgaria," said Genov, a blogger and political analyst. He knows his data was compromised because, though he's not an IT expert, he managed to find the stolen files online.

The attack is extraordinary, but it is not unique.

Government databases are gold mines for hackers. They contain a huge wealth of information that can be "useful" for years to come, experts say.

"You can make (your password) longer and more sophisticated, but the information the government holds are things that are not going to change," said Guy Bunker, an information security expert and the chief technology officer at Clearswift, a cybersecurity company.

"Your date of birth is not going to change, you're not going to move house tomorrow," he said. "A lot of the information that was taken was valid yesterday, is valid today, and will probably be valid for a large number of people in five, 10, 20 years' time."

Hackers' paradise

Data breaches used to be spearheaded by highly skilled hackers. But it increasingly doesn't take a sophisticated and carefully planned operation to break into IT systems. Hacking tools and malware that are available on the dark web make it possible for amateur hackers to cause enormous damage.

A strict data protection law that came into effect last year across the European Union has placed new burdens on anyone who collects and stores personal data. It also introduced hefty fines for anyone who mismanages data, potentially opening the door for the Bulgarian government to fine itself for the breach.

Still, attacks against government systems are on the rise, said Adam Levin, the founder of CyberScout, another cybersecurity firm. "It's a war right now -- one we will win if we make cybersecurity a front-burner issue," he said.

The notion that governments urgently need to step up their cybersecurity game is not new. Experts have been ringing alarm bells for years.

The US Department of Veterans Affairs suffered one of the first major data breaches in 2006, when personal data of more than 26 million veterans and military personnel were compromised.

"And it was all, 'Oh, this is dreadful. We must do things to stop it.' ... And here we are, 13 years later, and an entire country's data has been compromised, and in between, there's been incidents of large swathes of citizen data being compromised in different countries," Bunker said.

Out-of-date systems are often the problem. Some governments may have used private companies to manage the data they collected before the array of hacks and breeches brought their attention to cybersecurity.

"In many cases, our data was sent to third-party contractors years ago," Levin said. "The way we looked at data management 10 years ago seems antiquated today, yet that old data is still out there being managed by third parties, using legacy systems."

If the "old data" hasn't changed, it's still valuable to hackers.

The Bulgaria incident is concerning, said Desislava Krusteva, a Bulgarian privacy and data protection lawyer who advises some of the world's biggest tech companies on how to keep their clients' information safe.

"These kinds of incidents should not happen in a state institution. It seems like it didn't require huge efforts, and it's probably the personal data of almost all Bulgarian citizens," said Krusteva, a partner at Dimitrov, Petrov & Co., a law firm in Sofia.

The Bulgarian Commission for Personal Data Protection has said it would launch an investigation into the hack.

A National Revenue Agency spokesman would not comment on whether the data was properly protected.

"As there is undergoing investigation, we couldn't provide more details about reasons behind the hack," Communications Director Rossen Bachvarov said.

'Very embarrassing for the government'

A 20-year-old cybersecurity worker has been arrested by the Bulgarian police in connection with the hack. The computer and software used in the attack led police to the suspect, according to the Sofia prosecutor's office.

The man has been detained, and the police seized his equipment, including mobile phones, computers and drives, the prosecutor's office said in a statement. If convicted, he could spend as long as eight years in prison.

"It's still too early to say what exactly happened, but from political perspective, it is, of course, very embarrassing for the government," Krusteva said.

The embarrassment is made worse by the fact that this was not the first time the Bulgarian government was targeted. The country's Commercial Registry was brought down less than a year ago by an attack.

"So, at least for a year, the Bulgarian society, politicians, those who are in charge of the country, they knew quite well about the serious cybersecurity problems in the government infrastructures," Genov said, "and they didn't do anything about it."

Source: https://edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/index.html

2. Dating App Jack’d Fined After Leaking Users’ Nude Pics

LGBQT dating app Jack’d has been slapped with a $240,000 fine on the heels of a data breach that leaked personal data and nude photos of its users.

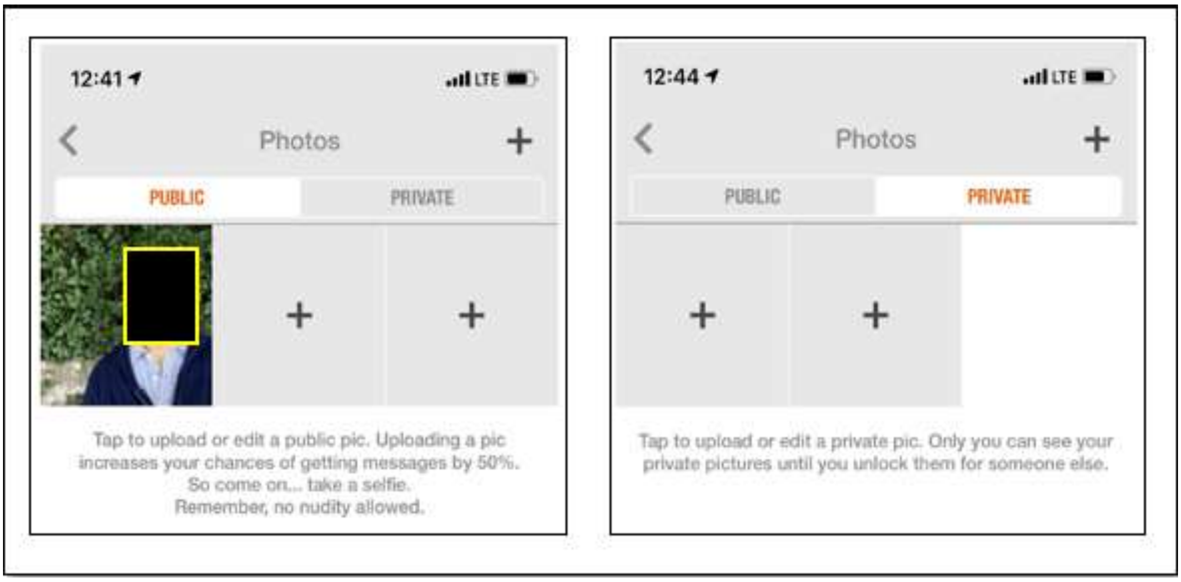
LGBTQ dating app Jack’d must cough up a $240,000 fine and “make substantial changes to improve security” on the heels of a security faux pas that leaked the private data – including nude photos – of thousands of its users.

Jack’d is a popular location-based app that caters to gay and bisexual men, which said it has more than 5 million users globally. The app’s parent company, Online Buddies, came under fire – and a subsequent investigation by the New York State Attorney General’s office – after reports emerged in February 2019 that it had left images of almost 2,000 users exposed via an insecure Amazon Web Services Simple Storage Service (S3) bucket.

The exposed data included user profile photos, nude pictures and user locations – information that could potentially put users at risk of arrest in certain countries. Making matters worse, the investigation concluded on Friday that though the company’s senior management team had been notified of the exposure in February 2018 by security researcher Oliver Hough, who discovered the issue, the company did not fix the misconfiguration until a year later, after media reports began shedding light on the data incident.

When asked about the Friday fine imposed on the dating app, Hough told Threatpost: “I think the result was a great message to send out to companies who blatantly don’t take privacy seriously.” That said, “It would be nice to see researchers rewarded for honest good faith effort like in my case; I made a whopping €0 from the whole thing, but ended up putting a lot of time into it answering emails and phone calls from the DAs office,” he said.

The Jack’d app gave users the choice to post photos on a public page viewable to all users, or on a private page that is only viewable to those that the app user picks. On this private page, the app allowed nude photos with the promise to users that it took “reasonable precautions” to protect their personal information from unauthorized access.



Tap to upload or edit a public pic. Uploading a pic increases your chances of getting messages by 50%. So come on... take a selfie. Remember, no nudity allowed.

Tap to upload or edit a private pic. Only you can see your private pictures until you unlock them for someone else.

Figure 1 Jack'd app

Despite that, the investigation found that Online Buddies failed to secure the private photos and other data and instead left the data wide open for the taking in an open Amazon Web Services S3 bucket.

Data exposed also included Jack'd user's device ID, operating system version, last login date and hashed password and when they last used the app.

Hough told Threatpost that there is no way for an external party to tell if anyone had accessed the data. Online Buddies did not respond to a request for comment from Threatpost.

The February 2019 data exposure disclosure resulted in a subsequent investigation, which resulted in the company having to pay up $240,000 and make significant changes to improve security.

"This app put users' sensitive information and private photos at risk of exposure and the company didn't do anything about it for a full year just so that they could continue to make a profit," said Attorney General Letitia James in a statement last week. "This was an invasion of privacy for thousands of New Yorkers. Today, millions of people across the country — of every gender, race, religion, and sexuality — meet and date online every day, and my office will use every tool at our disposal to protect their privacy."

Dating apps continue to come under increased scrutiny for the level of personal data collected from users. According to a recent report by ProPrivacy, dating apps like Match.com and Tinder collect location, chat message content and more personal data such as a history of recreational drug use, income level, sexual preferences, religious views and so on.

Meanwhile, other dating apps have gone through their own security issues. In February, a critical flaw was disclosed in the OkCupid app that could allow a bad actor to steal credentials, launch man-in-the-middle attacks or completely compromise the victim's application; and also in February dating app Coffee Meets Bagel warned users that it had been hit with a data breach.

Source: https://threatpost.com/dating-app-jackd-fined-after-leaking-users-nude-pics/146140/

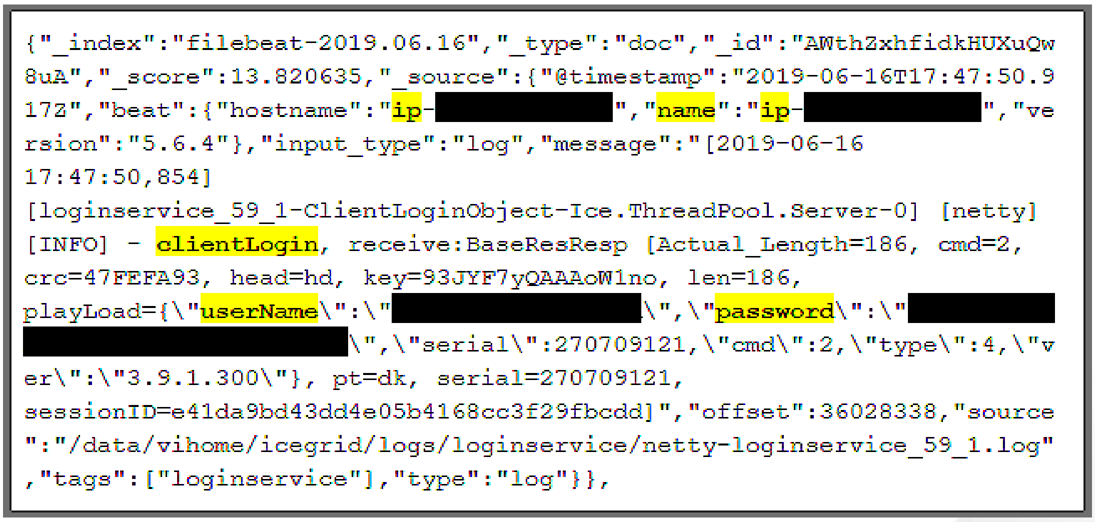
3. Billions of Records Including Passwords Leaked by Smart Home Vendor

Update: Orvibo secured their Elasticsearch server and sent us details on the measures taken after receiving vpnMentor's report (the response is attached at the end of the story).

A publicly accessible ElasticSearch cluster owned by Orvibo, a Chinese smart home solutions provider, leaked more than two billion user logs containing sensitive data of customers from countries all over the world.

Orvibo provides its clients with smart solutions designed to help them manage houses, offices, and hotel rooms via smart systems that offer security and energy management, as well as remote control and data recording/analysis using a smart home cloud platform.

Among the devices Orvibo's smart home solutions allow its users to control, the company's cloud platform comes with support for interaction center, smart lighting, home security, HVAC, energy management, and home entertainment devices.



```
{"_index":"filebeat-2019.06.16","_type":"doc","_id":"AWthZxhfidkHUXuQw
8uA","_score":13.820635,"_source":{"@timestamp":"2019-06-16T17:47:50.9
17Z","beat":{"hostname":"ip-[redacted]","name":"ip-[redacted]","ve
rsion":"5.6.4"},"input_type":"log","message":"[2019-06-16
17:47:50,854]
[loginservice_59_1-ClientLoginObject-Ice.ThreadPool.Server-0] [netty]
[INFO] - clientLogin, receive:BaseResResp [Actual_Length=186, cmd=2,
crc=47FEFA93, head=hd, key=93JYF7yQAAAoW1no, len=186,
playLoad={\"userName\":\"[redacted]\",\"password\":\"[redacted]
\",\"serial\":270709121,\"cmd\":2,\"type\":4,\"v
er\":\"3.9.1.300\"}, pt=dk, serial=270709121,
sessionID=e41da9bd43dd4e05b4168cc3f29fbcdd]","offset":36028338,"source
":"/data/vihome/icegrid/logs/loginservice/netty-loginservice_59_1.log"
,"tags":["loginservice"],"type":"log"}},
```

Figure 2 Sample of Orvibo leaked data

The exposed Orvibo database "includes over 2 billion logs that record everything from usernames, email addresses, and passwords, to precise locations" and it's still online given that the company did not respond to vpnMentor's research team who reached out on June 16.

As the researchers also state, "as long as the database remains open, the amount of data available continues to increase each day," with users from all over the world including

China, Japan, Thailand, the US, the UK, Mexico, France, Australia, and Brazil being affected by the data leak.

Among the customer data exposed by the unprotected Elasticsearch cluster were:

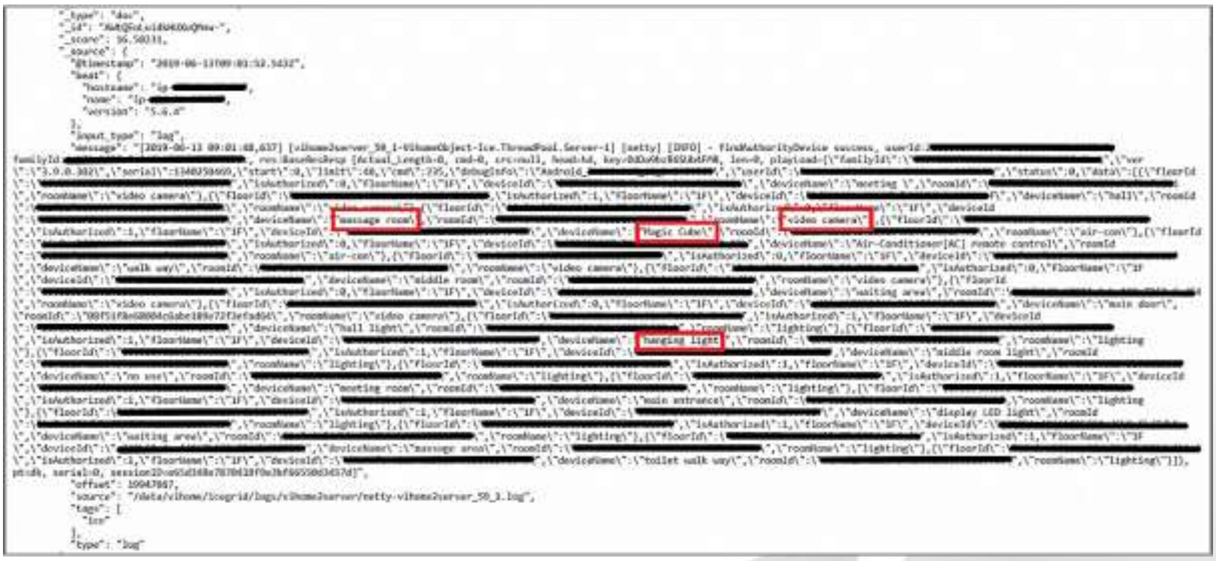
- Email addresses
- Passwords
- Account reset codes
- Precise user geolocation
- IP addresses
- Username & UserID
- Family name & Family ID
- Device name & Device that accessed account
- Recorded conversations through Smart Camera
- Scheduling information

The database leaked account reset codes that might allow potential attackers to lock Orvibo users out of their accounts without the need of using the users' passwords in the process.

To make things even worse, by changing both the password and the email address, the account could be unrecoverable providing hackers with "full control of their smart home devices."

The vpnMentor research team found that "the video feed from the smart cameras is easily accessible by entering the owner’s account with the credentials found in the database" for users who added security cameras to their Orvibo smart home management accounts.

Also, unlocking the users' smart door locks combined with precise geolocation and schedules swiped from built-in calendar displays exposes them to home break-ins.



```
      "_type": "doc",
      "_id": "AWtQFoLs1dU6DOuQHna-",
      "_score": 56.50031,
      "_source": {
        "@timestamp": "2019-06-13T09:01:52.543Z",
        "beat": {
          "hostname": "ip-[redacted]",
          "name": "ip-[redacted]",
          "version": "5.6.0"
        },
        "input_type": "log",
        "message": "[2019-06-13 09:01:48,637] [vihome2server_50_1-ViHomeObject-Ice.ThreadPool.Server-1] [netty] [INFO] - FindAuthorityDevice success, userId:[redacted]
familyId:[redacted], res:BaseResResp [Actual_Length=0, cmd=0, crc=null, head=hd, key=[illegible], len=0, playload={\"familyId\":\"[redacted]\",\"ver
\":\"3.0.0.302\",\"serial\":1340258609,\"start\":0,\"limit\":60,\"cmd\":235,\"debugInfo\":\"Android_[redacted]\",\"userId\":\"[redacted]\",\"status\":0,\"data\":[{\"floorId
\":\"[redacted]\",\"isAuthorized\":0,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"meeting \",\"roomId\":\"[redacted]
\",\"roomName\":\"video camera\"},{\"floorId\":\"[redacted],\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted]f\",\"deviceName\":\"hall\",\"roomId
\":\"[redacted]\",\"roomName\":\"video camera\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":0,\"floorName\":\"1F\",\"deviceId
\":\"[redacted]\",\"deviceName\":\"massage room\",\"roomId\":\"[redacted]\",\"roomName\":\"video camera\",{\"floorId\":\"[redacted]
\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"Magic Cube\",\"roomId\":\"[redacted]\",\"roomName\":\"air-con\"},{\"floorId
\":\"[redacted]\",\"isAuthorized\":0,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"Air-Conditioner[AC] remote control\",\"roomId
\":\"[redacted]\",\"roomName\":\"air-con\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":0,\"floorName\":\"1F\",\"deviceId\":\"[redacted]
\",\"deviceName\":\"walk way\",\"roomId\":\"[redacted]\",\"roomName\":\"video camera\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":0,\"floorName\":\"1F
\",\"deviceId\":\"[redacted]\",\"deviceName\":\"middle room\",\"roomId\":\"[redacted]\",\"roomName\":\"video camera\"},{\"floorId
\":\"[redacted]\",\"isAuthorized\":0,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"waiting area\",\"roomId\":\"[redacted]
\",\"roomName\":\"video camera\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":0,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"main door\",
\"roomId\":\"[illegible]\",\"roomName\":\"video camera\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId
\":\"[redacted]\",\"deviceName\":\"hall light\",\"roomId\":\"[redacted]\",\"roomName\":\"lighting\"},{\"floorId\":\"[redacted]
\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted],\"deviceName\":\"hanging light\",\"roomId\":\"[redacted]\",\"roomName\":\"lighting
\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted],\"deviceName\":\"middle room light\",\"roomId
\":\"[redacted]\",\"roomName\":\"lighting\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted]
\",\"deviceName\":\"no use\",\"roomId\":\"[redacted]\",\"roomName\":\"lighting\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId
\":\"[redacted]\",\"deviceName\":\"meeting room\",\"roomId\":\"[redacted]\",\"roomName\":\"lighting\"},{\"floorId\":\"[redacted]
\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"main entrance\",\"roomId\":\"[redacted],\"roomName\":\"lighting
\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"display LED light\",\"roomId
\":\"[redacted]\",\"roomName\":\"lighting\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted]
\",\"deviceName\":\"waiting area\",\"roomId\":\"[redacted]\",\"roomName\":\"lighting\"},{\"floorId\":\"[redacted]\",\"isAuthorized\":1,\"floorName\":\"1F
\",\"deviceId\":\"[redacted]\",\"deviceName\":\"massage area\",\"roomId\":\"[redacted]\",\"roomName\":\"lighting\"},{\"floorId\":\"[redacted]
\",\"isAuthorized\":1,\"floorName\":\"1F\",\"deviceId\":\"[redacted]\",\"deviceName\":\"toilet walk way\",\"roomId\":\"[redacted]\",\"roomName\":\"lighting\"}]},
pt=dk, serial=0, sessionID=[illegible]]",
        "offset": 19947867,
        "source": "/data/vihome/icegrid/logs/vihome2server/netty-vihome2server_50_1.log",
        "tags": [
          "ice"
        ],
        "type": "log"
```

Figure 3 Sample Orvibo Smart Camera log

Even though there is a small upside to all this given that Orvibo hashed its users' passwords, unfortunately, they were hashed using MD5 without salt which means that they could easily be cracked by a bad actor who gets his hands on them, subsequently taking control of the accounts.

"If Orvibo had added salt to their hashed passwords, it would have created a more complex string that is far more difficult to crack," says vpnMentor's report.

Securing ElasticSearch servers

Publicly-accessible ElasticSearch servers are constantly being discovered despite the core security features of the Elastic Stack becoming free according to an announcement made by Elastic NV on May 20.

"This means that users can now encrypt network traffic, create and manage users, define roles that protect index and cluster level access, and fully secure Kibana with Spaces" as per ElasticSearch's developers.

As ElasticSearch's developers also detailed back in December 2013, Elastisearch clusters should only be accessible by users on the local network to make sure that only the owners of the databases can access them.

Elastic NV also urges admins to secure the ElasticSearch stack by "encrypting communications, role-based access control, IP filtering, and auditing," to configure passwords for their servers' built-in users, as well as to properly configure the cluster before to deploying it.

While vpnMentor's research team contacted Orbivo to get the database down before publicly disclosing the data leak, we do not know if they also tried reaching out to CN-CERT to help them get in touch with the company and securing the DB — we asked vpnMentor if they did but had not received a response until this article was published.

BleepingComputer reached out to Orvibo and CN-CERT for comment and to secure the database but had not heard back at the time of this publication. This article will be updated when a response is received.

Update July 04 07:59 EDT: Orvibo secured the database and responded with the following statement:

Once we received this report on July 2nd, ORVIBO's RD team took immediate actions to resolve security vulnerability.

As an IoT company, ORVIBO attached great importance to user data security. We have taken effective solutions to resolve it:

1. Resolved security vulnerability.

2. Upgraded encryption mechanism of password.

3. Upgrade the protection on users account and password resetting.

4. Strengthening cooperation with professional cyber security companies to improve our system security.

Thanks for vpnMentor's research report. Due to their timely report, there has no any users' data leak until now. ORVIBO keeps improving users' data protection and information security in the long term.

Source: https://www.bleepingcomputer.com/news/security/billions-of-records-including-passwords-leaked-by-smart-home-vendor/

4. Mac Malware Pushed via Google Search Results, Masking as Flash Installer

A new malware is targeting Macs with new tactics to sniff out antivirus and virtual machines.

Never-before-seen Mac malware, dubbed OSX/CrescentCore, has been discovered in the wild. The trojan, spotted on various websites masquerading as an Adobe Flash Player installer, drops malicious applications and browser extensions on victims' systems when downloaded.

OSX/CrescentCore is spread via various websites, where it is masqueraded as an Adobe Flash Player installer. However, the "installer" is actually a .dmg file (an Apple disk image) that delivers the malware.

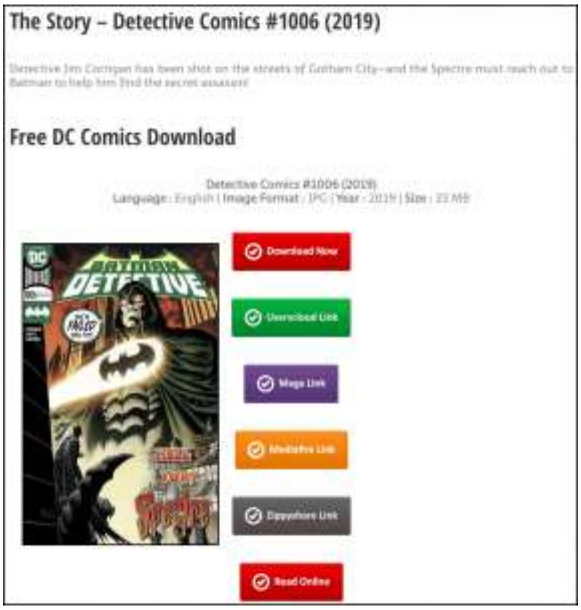
"One variant of OSX/CrescentCore was observed dropping potentially unwanted applications, rogue software like OSX/AMC (short for 'Advanced Mac Cleaner')," Joshua Long with Intego told Threatpost on Tuesday. "Another variant of OSX/CrescentCore tried to install a malicious Safari browser extension."

The malware was discovered by researchers being distributed via numerous sites – some of which popped up on Google search results. One such site, called "GetComics," purported to share digital copies of new comic books for free.

The malware was also spread via high-ranking Google search results, which were observed redirecting users to multiple sites.

"We were actually in the process of coming up with a name for CrescentCore, and searched for 'CrescentCore' in quotation marks, and one of the links in the first page of search results redirected to a page that happened to be distributing a new sample of CrescentCore," Long said.

The researcher said that oftentimes malware distributors will find vulnerable blogs or other sites with high Google search engine rankings, and add a redirection mechanism that bounces through a number of affiliate links – ultimately redirecting users to a fake Flash Player landing page.



The Story – Detective Comics #1006 (2019)

Detective Jim Corrigan has been shot on the streets of Gotham City–and the Spectre must reach out to Batman to help him find the secret assassin!

Free DC Comics Download

Detective Comics #1006 (2019)
Language : English | Image Format : JPG | Year : 2019 | Size : 33 MB

Figure 4 OSX CrescentCore pirated comics infection vector

“So if a result for a previously almost unused word like CrescentCore happened to show up in search results, it’s extremely likely that other search results are poisoned with redirections to this malware as well,” he said.

After looking further into these search results, researchers found that a page (hosted at any of a large number of domains) was displaying an Adobe Flash Player update warning popup. When clicked, this popup distributed either the new OSX/CrescentCore malware or previously discovered OSX/Shlayer malware.

However, “Unlike the typical, everyday, fake Flash Player updater, OSX/CrescentCore has some extra capabilities in an effort to make it more difficult for antivirus software to detect, and more difficult for malware analysts to examine and reverse engineer,” according to Intego’s analysis published last week.

Once downloaded the malware touts advanced features allowing it to skirt detection, including the capability to sniff out whether it’s running within a virtual machine environment (a common way to check machines for malware) or if antivirus software is present on the machine – if either are determined, it will simply shut down.

“Malware analysts often examine malware inside a VM to avoid unintentionally infecting their own computers while working with dangerous files, so malware authors sometimes implement VM detection and behave differently to make it more difficult to analyze the malware’s behavior,” said researchers.

If neither are detected, the malware will then install a LaunchAgent which helps it achieve persistence even further on the infected machine. LaunchAgent, which is a folder that can be installed in Macs’ Library folder that specifies code that should be run every time that user logs in, is commonly utilized by malware to achieve persistence on macOS.

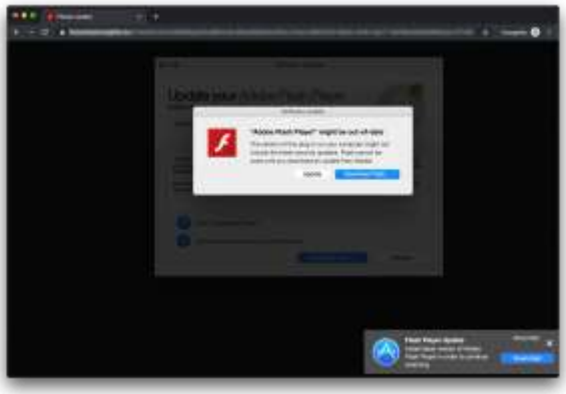


Figure 5 OSC CrescentCore fake Adobe Flash Player distribution site

The malware is signed using multiple Apple Developer IDs registered to someone named Sanela Lovic; known identifiers so far include 5UA7HW48Y7 and D4AYX8GHJS, said researchers.

The malware is only the latest discovered to be targeting Mac systems. Last week, researchers said they have discovered never-before-seen Mac malware samples (OSX/Linker) which they believe are being developed to target a recently-disclosed vulnerability in the MacOS operating system. In May, a bug was disclosed in the macOS security feature Gatekeeper that allows malicious code execution on systems running the most recent version of Mojave (10.14.0).

"Mac malware developers are actively becoming more clever, attempting to make it harder to detect the malicious nature of their software," said Long. "As we learned with OSX/Linker, makers of Mac malware are also experimenting with new ways of bypassing Apple's built-in protection mechanisms, even attempting to use zero-day vulnerabilities to do so."

Source: https://threatpost.com/mac-malware-pushed-via-google-search-results-masquerades-as-flash-installer/146178/

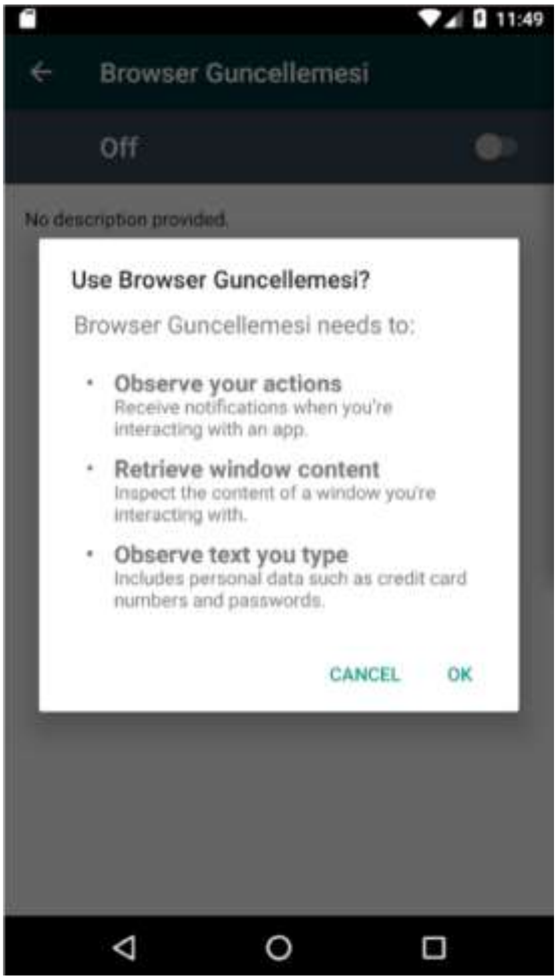
5. BianLian Android Banking Trojan Upgraded With Screen Recorder

The BianLian banking Trojan has been upgraded with two new modules designed to record the screens of infected Android devices and to create a SSH server for camouflaging its communication channels.

While BianLian was initially developed as a lowly dropper designed to be a transport conduit for more capable Android malware as observed by ThreatFabric's researchers during 2018, its developers eventually added several new modules that converted it into a banking Trojan.

The extra components allow the malware to send text messages, to run arbitrary USSD codes, to lock the screens of compromised devices, and to inject push notifications and perform overlay attacks that enable it to steal banking credentials.

FortiGuard Labs researchers have now discovered yet another BianLian sample that has been further upgraded by its masters, distributed in the form of a heavily obfuscated APK that relies "on generating a variety of random functions to hide the real functionalities of the sample."



No description provided.

Use Browser Guncellemesi?

Browser Guncellemesi needs to:

- Observe your actions
  Receive notifications when you're interacting with an app.
- Retrieve window content
  Inspect the content of a window you're interacting with.
- Observe text you type
  Includes personal data such as credit card numbers and passwords.

Figure 6 Requesting permissions

However, they were able to circumvent the huge amount of useless classes with randomly generated names designed to discourage malware analysts and discovered the malware sample is part of the aforementioned BianLian malware family.

The FortiGuard Labs discovered after analyzing the sample's behavior that the first thing the malicious "application does is hide its icon and constantly requests permission to abuse Accessibility services functionalities until granted."

After tricking its victims to give it permissions to inspect window contents and to observe text such as card numbers and passwords typed into various Android apps, the BianLian

Trojan will load its modules, ready to abuse the Accessibility services on the compromised Android device.

BianLian will load both older modules present in previous versions of the malware and newly added components designed to expand its capabilities.

Old modules:

- text: send, receive, and log SMS messages
- ussd: run USSD codes and make calls
- injects: run overlay attacks, mostly on banking applications
- locker: lock the screen, rendering the device unusable for a user

New modules:

- screencast: record device screen
- socks5: create SSH server

The new Socks5 component allows the banking Trojan to "create a functioning SSH server on the device using JSCH (Java Secure Channel), a library that implements SSH2 in pure Java."

With the help of this server, BianLian will tunnel its command and control (C2) communication channels using a SSH proxy that employs port forwarding on port 34500 to conceal the C2 traffic from prying eyes.

The Screencast module enables the malware to record its victims' screens by creating a virtual display using the android.media.projection.MediaProjection Android package, with the recording being launched remotely after unlocking the device's screen.

New Screencast module

New Socks5 module

Figure 7 Malware modules

BianLian will also drop a malicious payload on infected Android devices which allows it to check if "Google Play Protect is active through the Google SafetyNet API."

"The added functionalities, even though not completely original, are effective and make this family a potentially dangerous one. Its code base and strategies put it on a par with the other big players in the banking malware space," concludes the FortiGuard Labs team.

A full list of indicators of compromise (IOCs) including malware and payload hashes, C2 server domains, and a list of targeted banking apps is provided by the researchers at the end of their BianLian malware analysis.

The number of Android users targeted by cybercriminals with banking malware saw an alarming 300% increase in 2018, with roughly 1.8 million of them being eventually impacted by at least one such attack during the last year as detailed by Kaspersky Lab in its "Financial Cyberthreats in 2018" report.

A subsequent mobile malware evolution report for 2018 also issued by Kaspersky Lab in March showed that while banking and dropper Trojans have seen a consistent increase in the number of unique samples detected, the Asacub and the Hqwar banking Trojans were the most prevalent.

Source: https://www.bleepingcomputer.com/news/security/bianlian-android-banking-trojan-upgraded-with-screen-recorder/

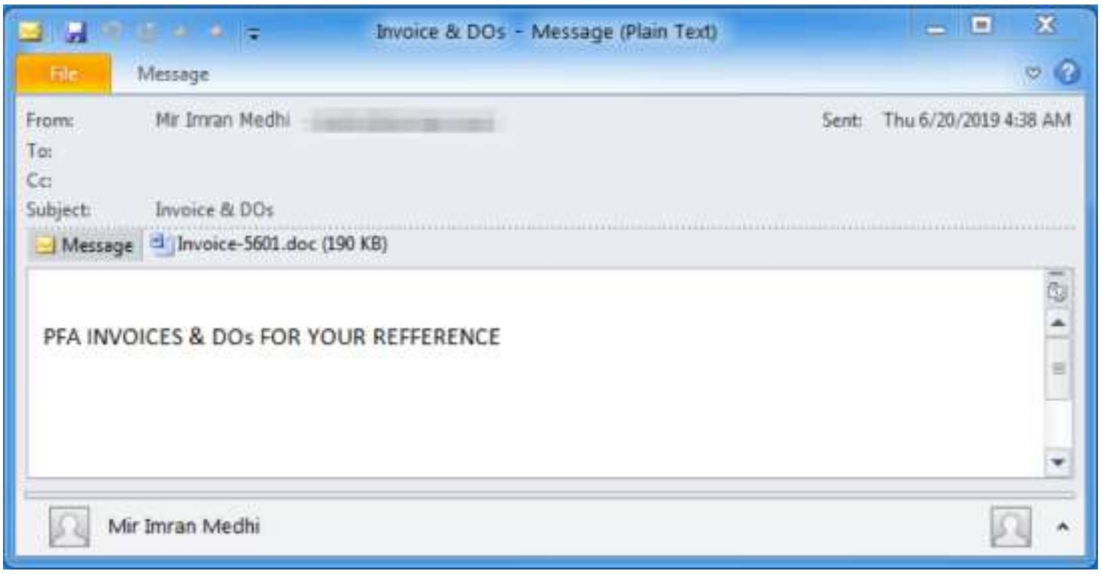
6. New Backdoor and Malware Downloader Used in TA505 Spam Campaigns

Several malicious spam campaigns are distributing new malware strains according to Trend Micro researchers, with the Gelup downloader and the FlowerPippi backdoor being used to attack targets from the Middle East, Japan, India, the Philippines, and Argentina.

Proofpoint researchers also discovered two spam campaigns distributing the malware downloader they dubbed AndroMut during June, with the attackers' crosshairs this time being set on recipients from U.S, Singapore, UAE, and South Korea.

The TA505 hacking group that was behind the Dridex banking trojan and Locky ransomware is also the one operating the seven campaigns seen by Trend Micro and the two observed by the Proofpoint team, with the new Gelup/AndroMut and FlowerPippi malware being added to the group's toolset starting with June.

TA505 used spam emails containing .DOC and .XLS documents to disseminate its new malware, with the payloads being dropped on compromised machines via VBA macros executed after opening the malicious attachments — a small number of spam samples also used malicious URLs leading to FlawedAmmyy RAT downloads according to Trend Micro.



From: Mir Imran Medhi [redacted]

Sent: Thu 6/20/2019 4:38 AM

To:

Cc:

Subject: Invoice & DOs

Message | Invoice-5601.doc (190 KB)

PFA INVOICES & DOs FOR YOUR REFFERENCE

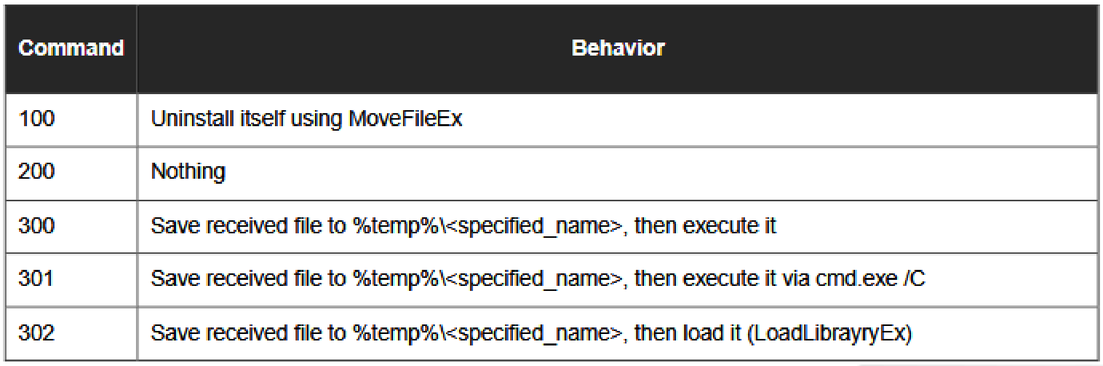
Mir Imran Medhi

Figure 8 Sample spam email (Proofpoint)

The new Gelup malware downloader's most interesting feature is that it uses obfuscation and an UAC-bypassing technique which is "mocking trusted directories (spoofing the file’s execution path in a trusted directory), abusing auto-elevated executables, and using the dynamic-link library (DLL) side-loading technique."

Gelup's developers also included various techniques designed to hinder static and dynamic analysis, as well as multiple deploying steps to make the infection process harder to track, as explained by Trend Micro in their technical analysis [PDF].

To gain persistence, Gelup would either schedule a task that launches a LNK file create in the system's Recycle Bin or add a registry run entry depending on the user privileges it has as explained by Proofpoint.



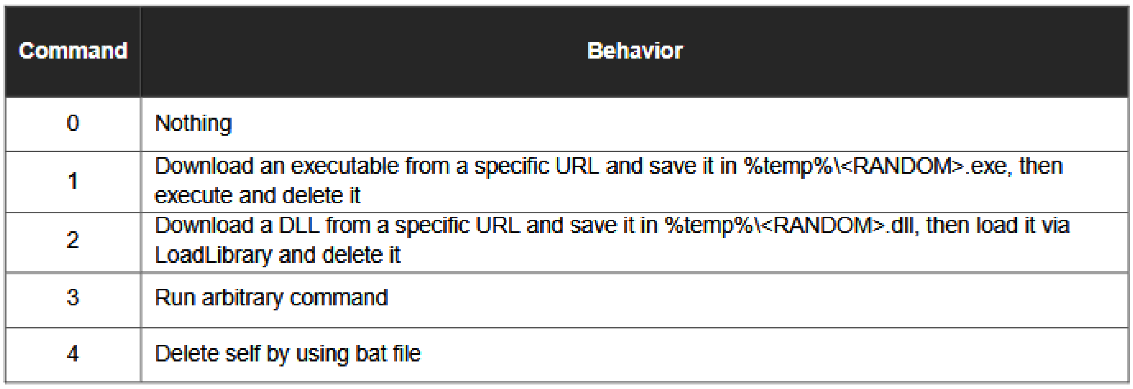
Command	Behavior
100	Uninstall itself using MoveFileEx
200	Nothing
300	Save received file to %temp%\<specified_name>, then execute it
301	Save received file to %temp%\<specified_name>, then execute it via cmd.exe /C
302	Save received file to %temp%\<specified_name>, then load it (LoadLibrayryEx)

Figure 9 Gelup commands (Trend Micro)

Proopfoint also said in their analysis of the downloader they dubbed AndroMut that it has "observed some low-confidence overlaps between it and two other malware downloaders: Andromeda and QtLoader. The research into the latter malware also noted some similarities to Andromeda."

FlowerPippi, the second malware recently deployed by TA505, also comes with downloader skills on top of its backdoor capabilities which enables it to drop more malicious payloads on infected systems in the form of executable binaries or DLL files.

As Trend Micro further points out, the backdoor is used to collect and exfiltrate information from its victims' computers, and to run arbitrary commands it receives from its command and control (C2) server.



Command	Behavior
0	Nothing
1	Download an executable from a specific URL and save it in %temp%\<RANDOM>.exe, then execute and delete it
2	Download a DLL from a specific URL and save it in %temp%\<RANDOM>.dll, then load it via LoadLibrary and delete it
3	Run arbitrary command
4	Delete self by using bat file

Figure 10 FlowerPippi commands (Trend Micro)

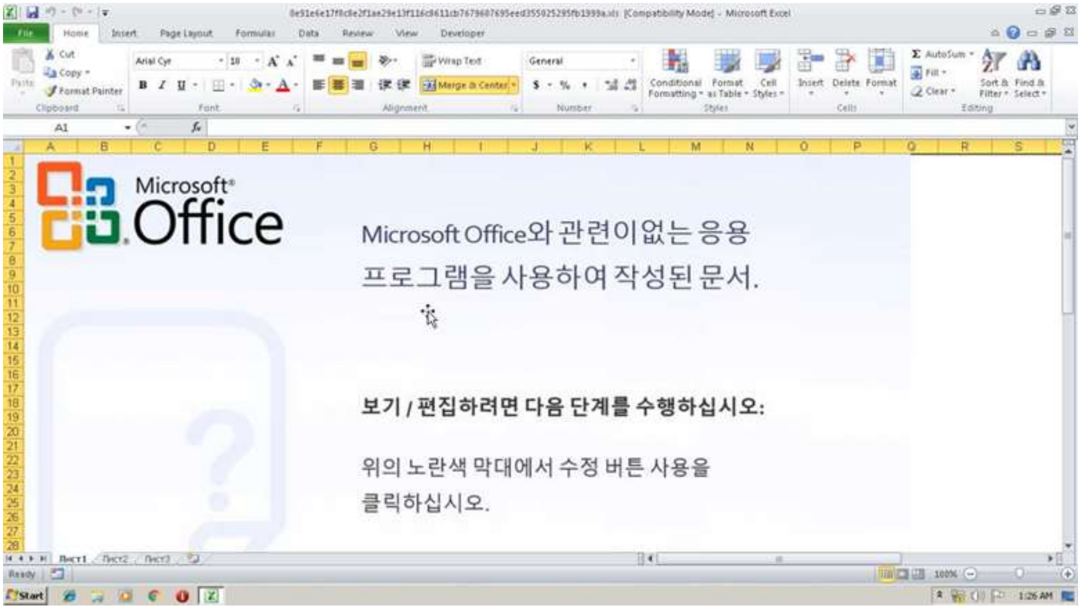
Ongoing TA505 campaigns

Besides the campaigns observed and documented by researchers from Proofpoint and Trend Micro, Microsoft Security Intelligence also issued an alert about two weeks ago about an active spam campaign that tries to infect Korean targets with a FlawedAmmyy RAT malware distributed via malicious XLS attachments.

While the CVE-2017-11882 Microsoft Office vulnerability exploited by the attackers was already patched by Microsoft two years ago, Redmond's researchers said that the exploit is still actively being used in attacks, with "increased activity in the past few weeks."

The FlawedAmmyy remote access Trojan payload is one of the favorite tools of the TA505 cybercriminal group which started dropping as part of its attacks against various targets.

Roughly a week earlier, Trend Micro's threat analysts detected a similar campaign to the one observed by the Microsoft researchers delivering the FlawedAmmyy RAT via malicious .XLS attachments, targeting South Korean users and attributed to the TA505 group.



Microsoft Office와 관련이없는 응용 프로그램을 사용하여 작성된 문서.

보기 / 편집하려면 다음 단계를 수행하십시오:

위의 노란색 막대에서 수정 버튼 사용을 클릭하십시오.

Figure 11 Malicious XLS document (Microsoft)

Ransomware, Trojans, and RATs on the menu

TA505 is a hacking group active since at least Q3 2014 [1, 2] with a known focus on attacking financial institutions and retail companies using large sized malicious spam campaigns disseminated via the Necurs botnet.

The group's malspam campaigns have distributed remote access Trojans (RATs) and malware downloaders that would drop the Dridex and Trick banking Trojans, as well as the Locky and Jaff ransomware strains on their targets' computers. [1, 2]

During November 2018, TA505 started distributing new malicious tools as seen by Proofpoint, with the ServHelper backdoor and the FlawedGrace remote access Trojan (RAT) being deployed as part of multiple malware campaigns directed at banks, retail businesses, and restaurants.

Indicators of compromise (IOCs) including malware sample hashes, domains, and URLs used by TA505 in their latest spam campaigns are provided by Trend Micro HERE and by Proofpoint HERE.

Microsoft also tweeted IOCs including hashes of the digitally signed executables and of the FlawedAmmyy RAT used in the campaign they detected.

Source: https://www.bleepingcomputer.com/news/security/new-backdoor-and-malware-downloader-used-in-ta505-spam-campaigns/

7. PGP Ecosystem Targeted in 'Poisoning' Attacks

A long-feared attack vector used against Pretty Good Privacy, the framework used to authenticate and keep email messages private, is being exploited for the first time. The attack, which takes aim at keyserver verification directories, makes it impossible for Pretty Good Privacy (PGP) to work properly for those targeted in attacks.

Unknown adversaries have singled out two recognized experts in the field of OpenPGP email encryption, Robert Hansen and Daniel Gillmor, in a series of targeted attacks. OpenPGP refers to the standard that uses the cryptographic privacy and authentication program PGP.

"In the last week of June 2019 unknown actors deployed a certificate spamming attack against two high-profile contributors in the OpenPGP community… This attack exploited a defect in the OpenPGP protocol itself in order to 'poison' [Hansen] and [Gillmor's] OpenPGP certificates," wrote Hansen in a technical description of the attacks.

The attack use undermines the complex mechanics used by OpenPGP. In a nutshell, the attack exploits Synchronizing Key Servers (SKS) that are used to help the discovery and distribution of public PGP digital certificates. Certificates are vital to how PGP works, in that they can be used to verify identity between two people. For added protection, people add signatures to certificates to further ensure a certificate is owned by the person who claims to own it.

What is exploited by attackers is the signature process. Within this framework, there are no limits to the number of signatures that a certificate can have. Generally, that's not an issue. However, in one of the popular implementation packages of OpenPGP, called GnuPG, attackers are exploiting a known "defect" where GnuPG cannot handle extremely high numbers of signatures very well.

Researchers call these signature-heavy certificates "poisoned".

"Anyone who attempts to import a poisoned certificate into a vulnerable OpenPGP installation will very likely break their installation in hard-to-debug ways," the researcher wrote. "Poisoned certificates are already on the SKS keyserver network. There is no reason to believe the attacker will stop at just poisoning two certificates."

Gillmor wrote last week on his personal blog that he was attacked. "My public cryptographic identity has been spammed to the point where it is unusable in standard workflows," he wrote.

Researchers believe now, given the ease and publicized success of the attacks, the number of poisoned certificates will escalate as copycat attacks spread.

"We've known for a decade this attack is possible. It's now here and it's devastating," Hansen wrote.

There is skepticism that the OpenPGP Working Group, who are tasked with maintaining the platform, will fix this issue in a reasonable timeframe. “Future releases of OpenPGP software will likely have some sort of mitigation, but there is no time frame. The best mitigation that can be applied at present is simple: stop retrieving data from the SKS keyserver network,” Hansen wrote.

Researchers say the problem of certificate poisoning and subsequent flooding of those certificates to the SKS has been known for years. Gillmor points out in his blog there have been proof-of-concept attacks and dire warnings.

“You can see discussion about this problem from a year ago along with earlier proposals for how to mitigate it. But none of those proposals have quite come to fruition, and people are still reliant on the SKS network,” he wrote.

As for temporary mitigation, Hansen said recommends: “At present I (speaking only for myself) do not believe the global keyserver network is salvageable. High-risk users should stop using the keyserver network immediately.”

Source: https://threatpost.com/pgp-ecosystem-targeted-in-poisoning-attacks/146240/

8. Microsoft Discovers Fileless Astaroth Trojan Campaign

A fileless malware campaign used by attackers to drop the information stealing Astaroth Trojan into the memory of infected computers was detected by Microsoft Defender ATP Research Team researchers.

The Astaroth Trojan and information stealer is a malware strain capable of stealing sensitive information such as user credentials from its victims using a key logger module, operating system calls interception, and clipboard monitoring.

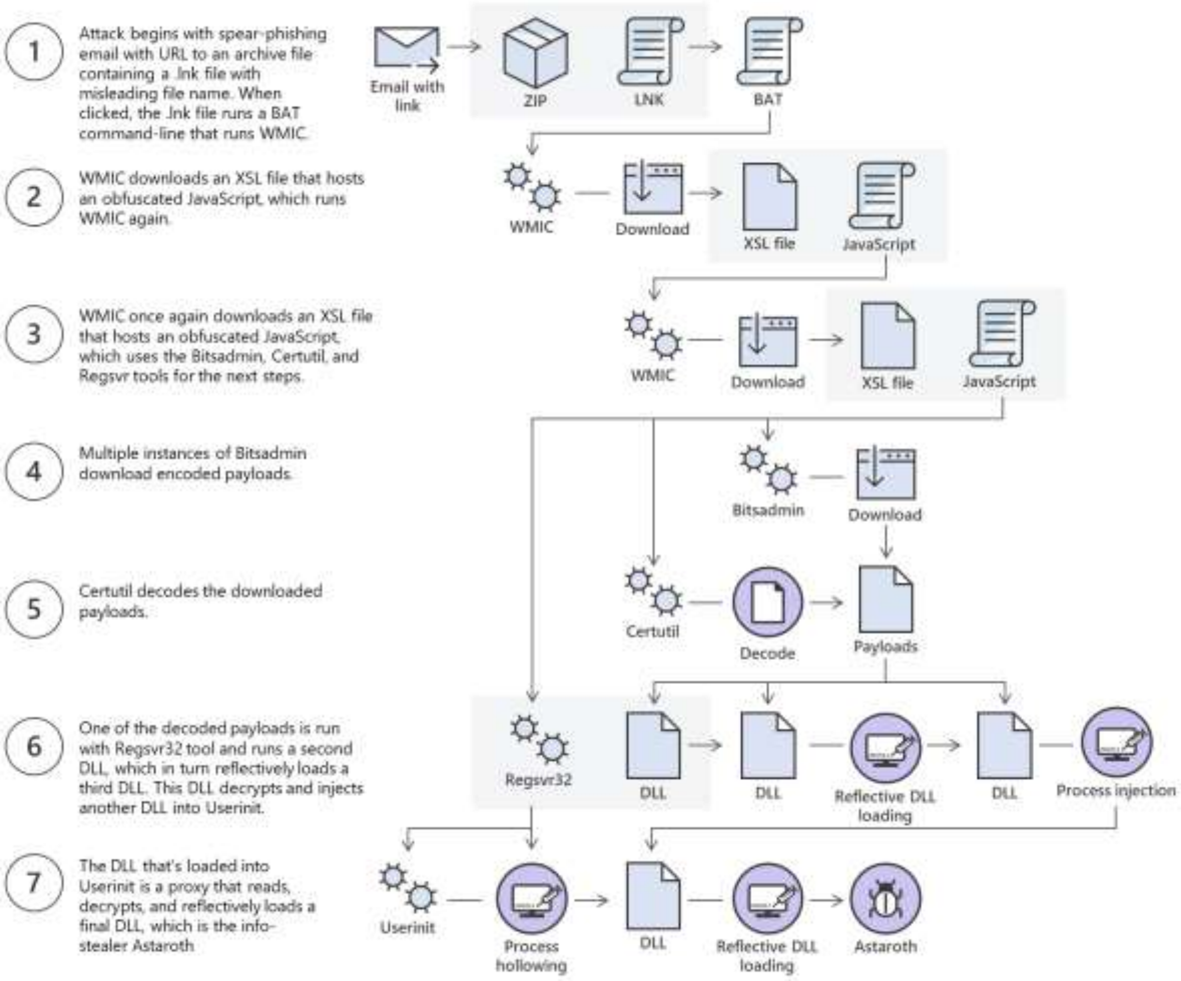
Astaroth is also known for abusing living-off-the-land binaries (LOLbins) such as the command line interface of the Windows Management Instrumentation Command-line (WMIC) to stealthily download and install malware payloads in the background.

The malware campaign discovered by the Microsoft Defender ATP Research Team uses several lifeless techniques and a multi-stage infection process that starts with a spear-phishing email containing a malicious link that leaded the potential victims to an LNK file.

After being double-clicked, "LNK file causes the execution of the WMIC tool with the “/Format” parameter, which allows the download and execution of a JavaScript code. The JavaScript code in turn downloads payloads by abusing the Bitsadmin tool."

The malicious payloads downloaded in the background are all Base64-encoded and get decoded on the compromised systems using the legitimate Certutil tool in the form of four DLLs that will be loaded with the help of the Regsvr32 tool.

The loaded DLL file will subsequently load a second DLL in memory that will reflectively load a third one, designed to decrypt and inject yet another DLL into Userinit. This fourth DLL acts as a proxy which will reflectively load a fifth DLL into memory using process hollowing.



1 Attack begins with spear-phishing email with URL to an archive file containing a .lnk file with misleading file name. When clicked, the .lnk file runs a BAT command-line that runs WMIC.

2 WMIC downloads an XSL file that hosts an obfuscated JavaScript, which runs WMIC again.

3 WMIC once again downloads an XSL file that hosts an obfuscated JavaScript, which uses the Bitsadmin, Certutil, and Regsvr tools for the next steps.

4 Multiple instances of Bitsadmin download encoded payloads.

5 Certutil decodes the downloaded payloads.

6 One of the decoded payloads is run with Regsvr32 tool and runs a second DLL, which in turn reflectively loads a third DLL. This DLL decrypts and injects another DLL into Userinit.

7 The DLL that's loaded into Userinit is a proxy that reads, decrypts, and reflectively loads a final DLL, which is the info-stealer Astaroth

Figure 12 Multi-stage infection process

This fifth and last DLL file is the final Astaroth infostealer Trojan malware payload that will collect and exfiltrate various types of sensitive info from its victims to command-and-control (C2) servers controlled by the attackers.

"It's interesting to note that at no point during the attack chain is any file run that's not a system tool. This technique is called living off the land: using legitimate tools that are already present on the target system to masquerade as regular activity," added the researchers.

Microsoft's researchers describe only the initial and execution stages of the malware attack in their report given that they only focused on how the Trojan infection was detected and blocked by Microsoft Defender ATP.

The defense features and technologies used by Microsoft Defender ATP to stop the infection are detailed in a graph detailing stage-by-stage the solutions used to identify and prevent an Astaroth infection on affected Windows computers.

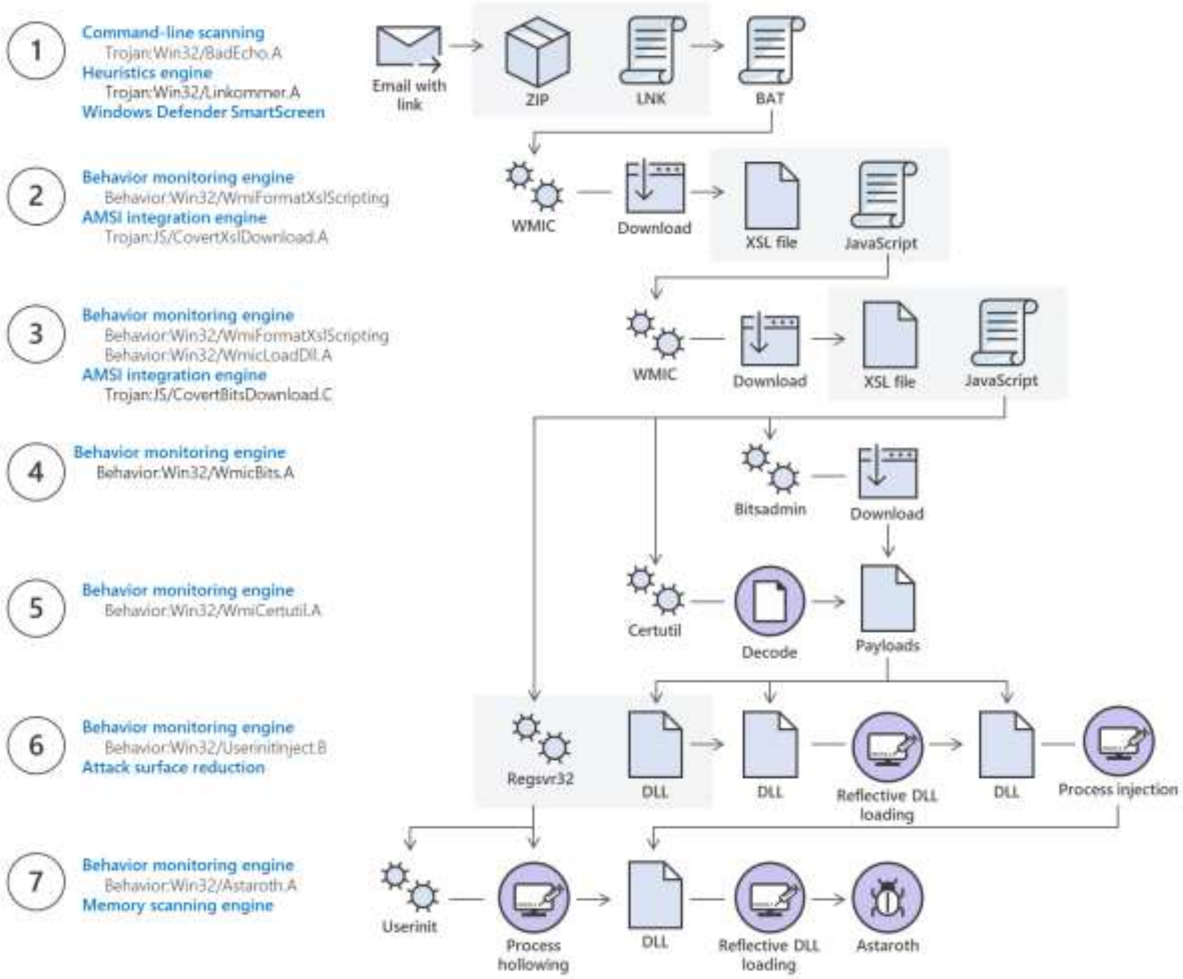

1
Command-line scanning
Trojan:Win32/BadEcho.A
Heuristics engine
Trojan:Win32/Linkommer.A
Windows Defender SmartScreen
Email with link
ZIP
LNK
BAT
2
Behavior monitoring engine
Behavior:Win32/WmiFormatXslScripting
AMSI integration engine
Trojan:JS/CovertXslDownload.A
WMIC
Download
XSL file
JavaScript
3
Behavior monitoring engine
Behavior:Win32/WmiFormatXslScripting
Behavior:Win32/WmicLoadDll.A
AMSI integration engine
Trojan:JS/CovertBitsDownload.C
WMIC
Download
XSL file
JavaScript
4
Behavior monitoring engine
Behavior:Win32/WmicBits.A
Bitsadmin
Download
5
Behavior monitoring engine
Behavior:Win32/WmiCertutil.A
Certutil
Decode
Payloads
6
Behavior monitoring engine
Behavior:Win32/UserinitInject.B
Attack surface reduction
Regsvr32
DLL
DLL
Reflective DLL loading
DLL
Process injection
7
Behavior monitoring engine
Behavior:Win32/Astaroth.A
Memory scanning engine
Userinit
Process hollowing
DLL
Reflective DLL loading
Astaroth

Figure 13 Blocking Astaroth's fileless techniques

Microsoft Defender ATP Research Team also enumerates the techniques used in the Astaroth fileless malware attack on each infection stage and the Windows tools employed to stealthily spread the infection on compromised systems.

As Microsoft Defender ATP Research's Andrea Lelli concluded, "abusing fileless techniques does not put malware beyond the reach or visibility of security software. On the contrary, some of the fileless techniques may be so unusual and anomalous that they draw immediate attention to the malware, in the same way that a bag of money moving by itself would."

Back in February, another Astaroth campaign was observed by Cybereason while exploiting security and anti-malware solutions, as well as living-off-the-land techniques and abusing living-off-the-land binaries (LOLbins) to steal information from European and Brazilian targets.

Cofense's Phishing Defense Center (PDC) also spotted a malspam campaign distributing Astaroth in September 2018 and exclusively targeting South American victims, with around 8,000 machines potentially compromised within a single week of attacks.

Source: https://www.bleepingcomputer.com/news/security/microsoft-discovers-fileless-astaroth-trojan-campaign/

9. GoBotKR Targets Pirate Torrents to Build a DDoS Botnet

A botnet dubbed GoBotKR is targeting fans of Korean TV, compromising computers via pirated copies of South Korean movies, games and TV shows available via Korean and Chinese torrent sites. Ultimately, the cybercriminals are building a network that can then be used to perform DDoS attacks of various kinds, according to an analysis from ESET.

While the torrents purport to be pirate versions of real content, they actually contain two malicious files (with deceptive filenames, extensions and icons), in addition to the expected MP4 file. The first is a malicious executable masked as a PMA archive file, with a filename mimicking various codec installers, according to ESET. The second is a malicious LNK file with a filename and icon mimicking the expected video file.

Clicking on the latter executes the malware, while also opening the MP4 and playing the expected content.

“Directly opening the intended MP4 file will not result in any malicious action,” the researchers said in a posting on Monday. “The catch here is that the MP4 file is often hidden in a different directory, and users might encounter the malicious LNK file mimicking it first. Further increasing the chance of users falling for the lure is the fact that the extension of the LNK file is normally not displayed when viewed in Windows Explorer.”

After being executed, GoBotKR collects system information about the compromised computer, including network configuration, OS version information, CPU and GPU versions, along with a list of installed antivirus software. Researchers said that the intel is then sent to the command-and-control (C2) server, to help the attackers determine which bots should be used in various attacks.

GoBotKR can also receive a “seed torrents” command, allows the attackers to misuse the victimized machines for seeding arbitrary files using the BitTorrent and uTorrent programs: “This may be used as a mechanism to distribute the malware further,” researchers noted.

The malware is a revamped version of a known backdoor named GoBot2, according to ESET. The code is straightforward, they added, with most features implemented with the use of GoLang libraries, and by executing Windows commands and third-party utilities, such as BitTorrent and uTorrent clients.

"The modifications to the source code are mainly South Korea-specific evasion techniques," the researchers said. These include using the IP information of the compromised computer to detect whether it is running in Korean-specific security sandboxes; and, scanning running processes on the compromised system to detect selected antivirus products. If any of the products are detected, the malware terminates itself and removes some traces of its activity from the host. The list of detected processes includes products by AhnLab, a South Korean security company.

The botnet is indicative of a coding trend being used by threat actors, ESET researchers added. "Both the original and the modified version are written in GoLang, also known as Go," they said. "While still relatively rare for malware, new variants of GoLang malware are emerging, likely due to the challenges posed to analysts with the bulky nature of its compiled executables."

They added that since March 2018, GoBotKT has swelled in size (though they didn't quantify the number of compromised endpoints). The bots are located mostly in South Korea (80 percent), China (10 percent) and Taiwan (5 percent).

Pirated content has been a well-known vector for spreading all kinds of malware for quite some time. In April, Kaspersky released a report that found that illegal downloads of HBO's Game of Thrones accounted for 17 percent of all infected pirated content in the last year. And in Aug. 2018, researchers at ESET said they found DDoS modules had been added to a Kodi third-party add-on.

"To steer clear of similar attacks in the future, stick to official sources when downloading content," according to ESET. "Before launching downloaded files, pay attention to whether their extensions match the intended filetypes. To keep your computer protected, we advise you to patch regularly and use reputable security software."

Source: https://threatpost.com/gobotkr-pirate-torrents-ddos-botnet/146285/

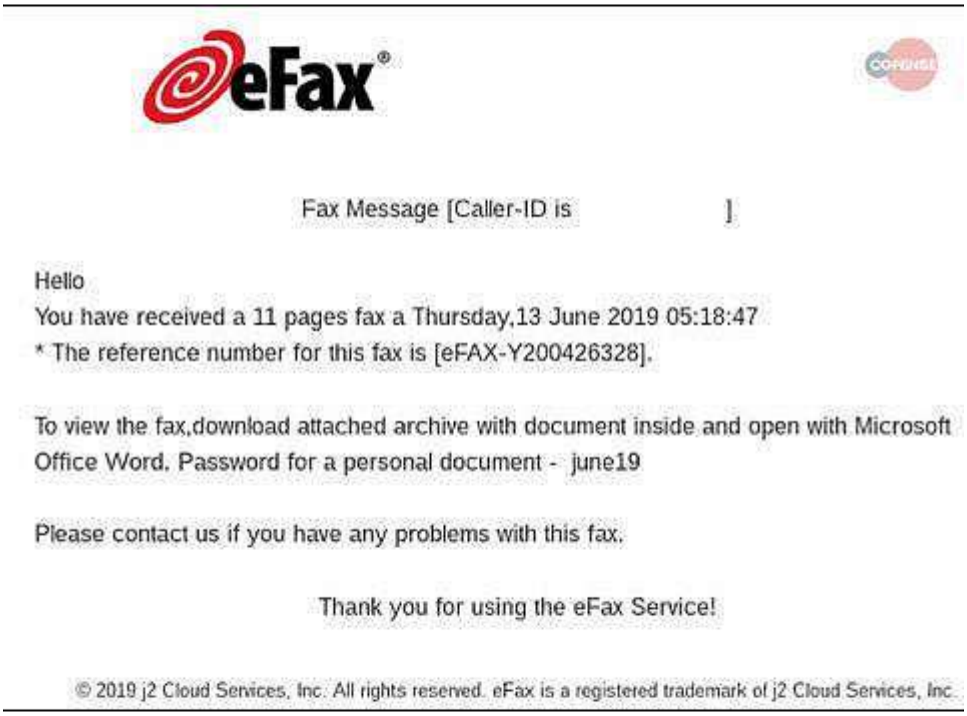
10. Dridex Banking Trojan, RMS RAT Dropped via Fake eFax Messages

Researchers from Cofense have discovered a new malspam campaign that delivers fake eFax messages designed to drop a banking Trojan and RAT cocktail via malicious Microsoft Word document attachments.

The phishing emails that impersonate eFax messages include ZIP archived XLS Microsoft Excel documents with a macro designed to download and launch Dridex and Remote Manipulator System Remote Access Tool (RMS RAT) malicious payloads.

The attackers use the two payloads to perform different tasks: the Dridex banking Trojan to collect credentials from web browsers and to exfiltrate them to their own servers, and the RMS RAT for managing the infected computers.

Cofense's research team also added that "And having both available provides a backup communication channel in case one of the malware families is detected and removed."



eFax®

Fax Message [Caller-ID is]

Hello
You have received a 11 pages fax a Thursday,13 June 2019 05:18:47
* The reference number for this fax is [eFAX-Y200426328].

To view the fax,download attached archive with document inside and open with Microsoft Office Word. Password for a personal document - june19

Please contact us if you have any problems with this fax.

Thank you for using the eFax Service!

© 2019 j2 Cloud Services, Inc. All rights reserved. eFax is a registered trademark of j2 Cloud Services, Inc.

Figure 14 Phishing email sample

While RMS RAT is actually a legitimate remote control utility, it has been adopted by bad actors and included in their toolkits because of its "logging keystrokes, recording from the webcam or microphone, transferring files, and manipulating Windows Task Manager and other Windows utilities" capabilities.

All these features allow malicious campaign operators to control compromised computers with ease once RMS RAT payload is dropped and system information such as IP addresses and login credentials are sent to their command-and-control (C2) servers.

As a bonus, since RMS RAT is a legitimate remote control software, most security and anti-malware solutions will not mark it as suspicious or malicious, allowing the attackers to go undetected and undergo all their nefarious tasks.

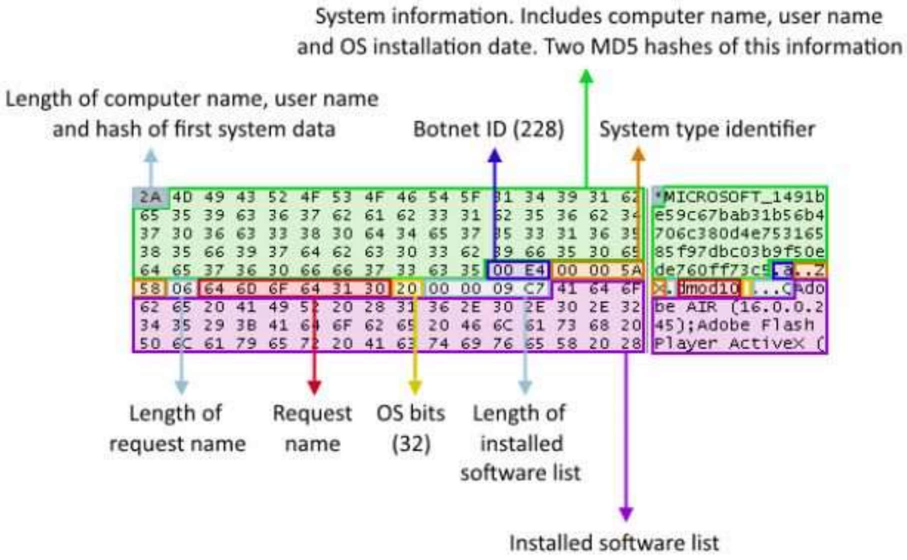
Web injects used to abuse victims' web browsers

Just as in the case of other banking Trojans, the Dridex strain disseminated via this malspam campaign also uses web injects in the form of scripts loaded by the infected machine when visiting a targeted website.

This is done by injecting the data-pilfering script into the web browser, making it possible for the malware to steal any info typed by the victim, as well as for more villainous purposes such as [bypassing security questions and multi-factor authentication](), and redirecting traffic.

"In this case, the web injects used by Dridex were unusual because of both the large number of possible web inject scripts and the fact that some of the web injects were labeled as being from the Zeus banking trojan," said the Cofense research team.

While some of the web injects used by the Dridex Trojan, in this case, are hardcoded within the malware, there's also one with more features that will be downloaded from a remote host on the compromised systems.



```
2A 4D 49 43 52 4F 53 4F 46 54 5F 31 34 39 31 62   *MICROSOFT_1491b
65 35 39 63 36 37 62 61 62 33 31 62 35 36 62 34   e59c67bab31b56b4
37 30 36 63 33 38 30 64 34 65 37 35 33 31 36 35   706c380d4e753165
38 35 66 39 37 64 62 63 30 33 62 39 66 35 30 65   85f97dbc03b9f50e
64 65 37 36 30 66 66 37 33 63 35 00 E4 00 00 5A   de760ff73c5.ä..Z
58 06 64 6D 6F 64 31 30 20 00 00 09 C7 41 64 6F   X.dmod10 ...ÇAdo
62 65 20 41 49 52 20 28 31 36 2E 30 2E 30 2E 32   be AIR (16.0.0.2
34 35 29 3B 41 64 6F 62 65 20 46 6C 61 73 68 20   45);Adobe Flash 
50 6C 61 79 65 72 20 41 63 74 69 76 65 58 20 28   Player ActiveX (
```

System information. Includes computer name, user name and OS installation date. Two MD5 hashes of this information
Length of computer name, user name and hash of first system data
Botnet ID (228)
System type identifier
Length of request name
Request name
OS bits (32)
Length of installed software list
Installed software list

Figure 15 Analysis of Dridex data header sent to a C2 server (Forcepoint)

Several types of sites targeted using multiple injects

The attackers use Dridex to target several types of sites, from cryptocurrency and banking websites to e-commerce websites, with web injects deployed from different command-and-control (C2) servers. Notably, some of the scripts used for the same websites are tagged as 'Zeus' injects, another banking Trojan used for information stealing.

The multiple types of web injects used in this campaign by the attackers allows them to "have a wide variety of possible targets at their disposal" and "target information even when the structure of the webpages' URL has changed over time" as explained by the Cofense researchers.

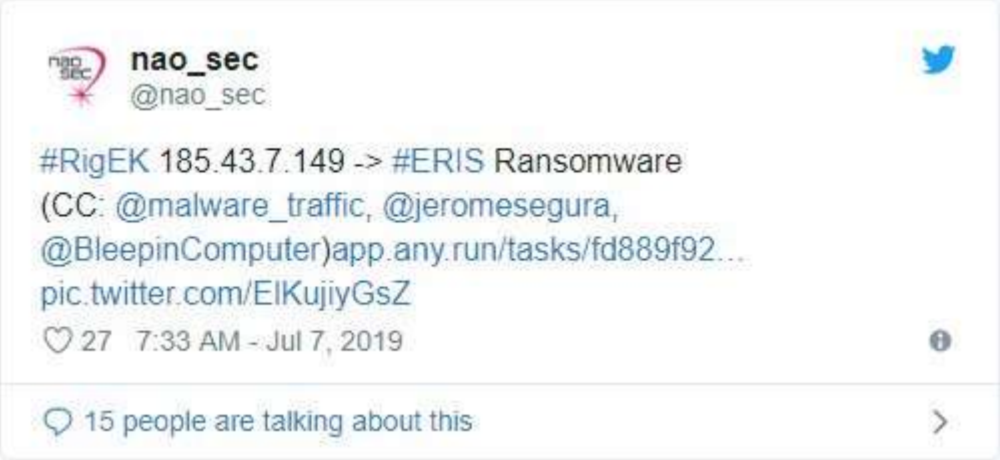
A full list of indicators of compromise (IOCs) including potential web inject sources, RMS RAT and Dridex C2 server domains, and payload URLs are available at the end of the [Cofense malspam campaign report]().

Source: https://www.bleepingcomputer.com/news/security/dridex-banking-trojan-rms-rat-dropped-via-fake-efax-messages/

11. Rig Exploit Kit Pushing Eris Ransomware in Drive-by Downloads

The RIG exploit kit has been spotted distributing the new ERIS Ransomware as its payload. Using the RIG exploit kit, vulnerable victims will find that the ransomware is installed on their computer without their knowledge simply by visiting a web site.

The ERIS ransomware was originally spotted in May 2019 by Michael Gillespie when it was submitted to his ID Ransomware site, but a sample was not available at the time. Over the weekend, exploit kit researcher nao sec spotted it being distributed through a malvertising campaign using the RIG exploit kit.



nao_sec
@nao_sec

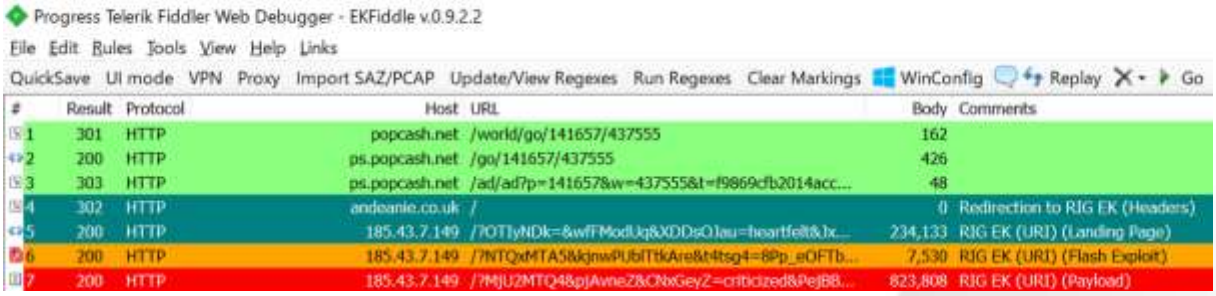
#RigEK 185.43.7.149 -> #ERIS Ransomware
(CC: @malware_traffic, @jeromesegura, @BleepinComputer)app.any.run/tasks/fd889f92...
pic.twitter.com/ElKujiyGsZ

♡ 27 7:33 AM - Jul 7, 2019

15 people are talking about this

Figure 16 nao_sec's tweet about the ERIS ransomware

According to nao_sec, a malvertising campaign using the popcash ad network is redirecting users to the RIG exploit kit. This is illustrated in the captured web requests shown below.



Progress Telerik Fiddler Web Debugger - EKFiddle v.0.9.2.2
File Edit Rules Tools View Help Links
QuickSave UI mode VPN Proxy Import SAZ/PCAP Update/View Regexes Run Regexes Clear Markings WinConfig Replay Go

#	Result	Protocol	Host	URL	Body	Comments
1	301	HTTP	popcash.net	/world/go/141657/437555	162	
2	200	HTTP	ps.popcash.net	/go/141657/437555	426	
3	303	HTTP	ps.popcash.net	/ad/ad?p=141657&w=437555&t=f9869cfb2014acc...	48	
4	302	HTTP	andeanie.co.uk	/	0	Redirection to RIG EK (Headers)
5	200	HTTP	185.43.7.149	/?OTIyNDk=&wfFModUq&XDDsOJau=heartfelt&Jx...	234,133	RIG EK (URI) (Landing Page)
6	200	HTTP	185.43.7.149	/?NTQxMTA5&kjnwPUbITtkAre&t4tsg4=8Pp_eOFTb...	7,530	RIG EK (URI) (Flash Exploit)
7	200	HTTP	185.43.7.149	/?MjU2MTQ4&pjAwneZ&CNxGeyZ=criticized&PejBB...	823,808	RIG EK (URI) (Payload)

Figure 17 Popcash Malvertising Campaign

When redirected to the exploit, nao_sec told BleepingComputer that the kit will attempt to exploit a Shockwave (SWF) vulnerability in the browser. If successful, it will automatically download and install the ERIS Ransomware on to the computer.

The ERIS Ransomware

When the ERIS Ransomware is installed, it will encrypt a victim's files and append the .ERIS extension as shown below.

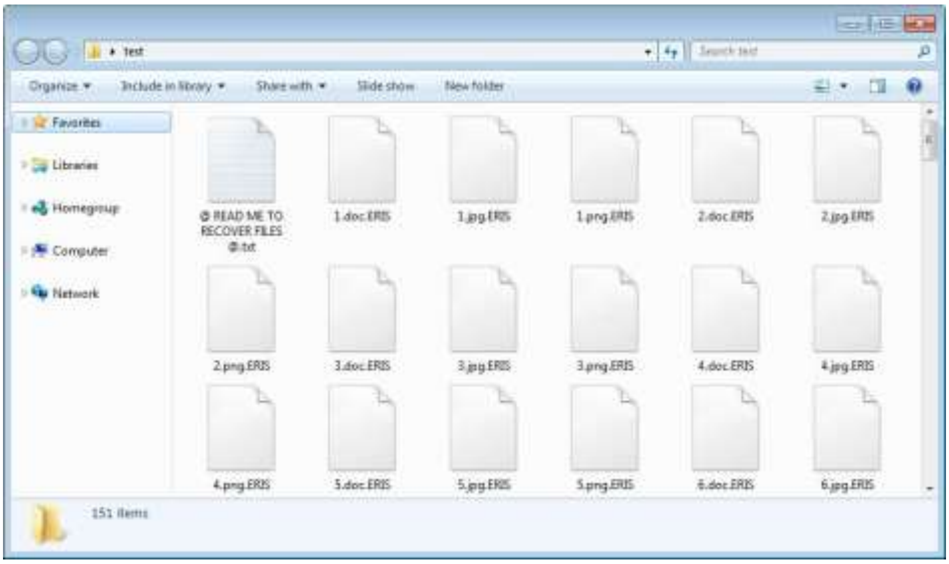
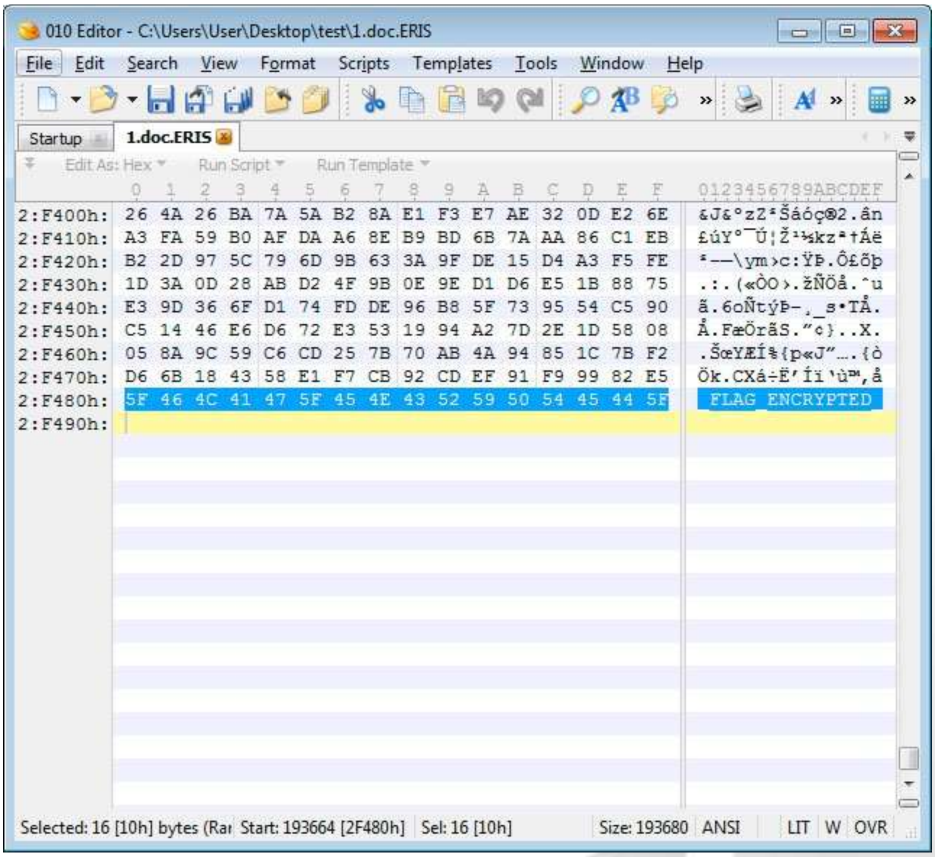


Figure 18 ERIS Encrypted Files

Each encrypted file contains a file marker of **_FLAG_ENCRYPTED_** at the end of the file to indicate it was encrypted by the ransomware.

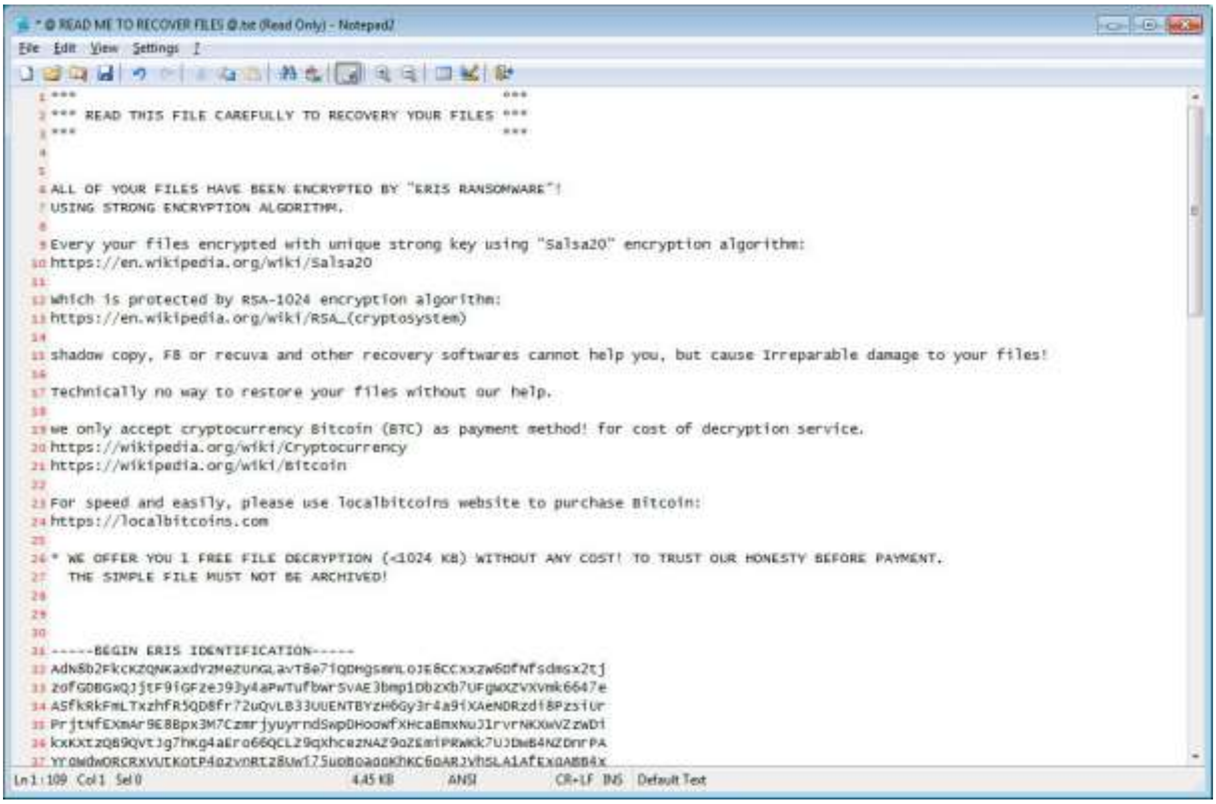


```
            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2:F400h:   26 4A 26 BA 7A 5A B2 8A E1 F3 E7 AE 32 0D E2 6E   &J&°zZ²Šáóç®2.ân
2:F410h:   A3 FA 59 B0 AF DA A6 8E B9 BD 6B 7A AA 86 C1 EB   £úY°¯Ú¦Ž¹½kzª†Áë
2:F420h:   B2 2D 97 5C 79 6D 9B 63 3A 9F DE 15 D4 A3 F5 FE   ²-—\ym›c:ŸÞ.Ô£õþ
2:F430h:   1D 3A 0D 28 AB D2 4F 9B 0E 9E D1 D6 E5 1B 88 75   .:.(«ÒO›.žÑÖå.ˆu
2:F440h:   E3 9D 36 6F D1 74 FD DE 96 B8 5F 73 95 54 C5 90   ã.6oÑtýÞ–¸_s•TÅ.
2:F450h:   C5 14 46 E6 D6 72 E3 53 19 94 A2 7D 2E 1D 58 08   Å.FæÖrãS.”¢}..X.
2:F460h:   05 8A 9C 59 C6 CD 25 7B 70 AB 4A 94 85 1C 7B F2   .ŠœYÆÍ%{p«J”….{ò
2:F470h:   D6 6B 18 43 58 E1 F7 CB 92 CD EF 91 F9 99 82 E5   Ök.CXá÷Ë’Íï‘ù™‚å
2:F480h:   5F 46 4C 41 47 5F 45 4E 43 52 59 50 54 45 44 5F   _FLAG_ENCRYPTED_
2:F490h:
```

Selected: 16 [10h] bytes (Rar Start: 193664 [2F480h] Sel: 16 [10h] Size: 193680 ANSI LIT W OVR

Figure 19 _FLAG_ENCRYPTED_ File Marker

In each folder that was scanned, the ransomware will also created a ransom note named **@ READ ME TO RECOVER FILES @.txt** that instructs the user victim to contact Limaooo@cock.li for payment instructions. Included in this ransom note is a unique ID that the victim must send to the ransomware developer so that they can perform a free test decryption of one file.



* @ READ ME TO RECOVER FILES @.txt (Read Only) - Notepad2
File Edit View Settings ?

```
***                                            ***
*** READ THIS FILE CAREFULLY TO RECOVERY YOUR FILES ***
***                                            ***


ALL OF YOUR FILES HAVE BEEN ENCRYPTED BY "ERIS RANSOMWARE"!
USING STRONG ENCRYPTION ALGORITHM.

Every your files encrypted with unique strong key using "Salsa20" encryption algorithm:
https://en.wikipedia.org/wiki/Salsa20

Which is protected by RSA-1024 encryption algorithm:
https://en.wikipedia.org/wiki/RSA_(cryptosystem)

shadow copy, FB or recuva and other recovery softwares cannot help you, but cause Irreparable damage to your files!

Technically no way to restore your files without our help.

We only accept cryptocurrency Bitcoin (BTC) as payment method! for cost of decryption service.
https://wikipedia.org/wiki/Cryptocurrency
https://wikipedia.org/wiki/Bitcoin

For speed and easily, please use localbitcoins website to purchase Bitcoin:
https://localbitcoins.com

* WE OFFER YOU 1 FREE FILE DECRYPTION (<1024 KB) WITHOUT ANY COST! TO TRUST OUR HONESTY BEFORE PAYMENT.
  THE SIMPLE FILE MUST NOT BE ARCHIVED!



-----BEGIN ERIS IDENTIFICATION-----
AdN8b2FkcKZQNKaxdY2MeZUnGLavT8e7iQDHgsmnLoJE8CCxxzw6DfNfsdmsx2tj
ZofGDBGxQJjtF9iGFzeJ93y4aPwTufbwr5vAE3bmp1Dbzxb7UFgWXZVXvmk6647e
ASfkRkFmLTxzhfR5QD8fr72uQvLB33UUENTBYzH6Gy3r4a9iXAeNDRzdi8PzsiUr
PrjtNfEXmAr9E8Bpx3M7CzmrjyuyrndSwpDHoowfXHcaBmxNuJ1rvrNKXWVZzwDi
kxKXtzQB9QvtJg7hKg4aEro66QCL29qXhcezNAZ9oZEmiPRWKk7UJDwB4NZDnrPA
YrOWdwORCRXVUtKotP4ozvnRtz8Uw175uoBoaogKhKC6oARJVh5LA1AfExoAB84x
```

Figure 20 ERIS Ransom Note

Unfortunately, at this time there is no way to decrypt files encrypted by ERIS for free. If anything changes, we will create a future article with any additional findings.

Source: https://www.bleepingcomputer.com/news/security/rig-exploit-kit-pushing-eris-ransomware-in-drive-by-downloads/

12. New eCh0raix Ransomware Brute-Forces QNAP NAS Devices

A new ransomware strain written in Go and dubbed eCh0raix by the Anomali Threat Research Team is being used in the wild to infect and encrypt documents on consumer and enterprise QNAP Network Attached Storage (NAS) devices used for backups and file storage.

Originally discovered by reports from victims in a BleepingComputer forum thread, the ransomware has been reported to target the following QNAP NAS devices: QNAP TS-231, QNAP TS-251, QNAP TS 253A, QNAP TS 253B, QNAP TS-451, and QNAP TS-459 Pro II.

According to Anomali researchers, these NAS devices are being attacked through weak credentials and by exploiting known vulnerabilities.

QNAP Systems, the manufacturer of QNAP NAS devices, provides a list of steps that could allow rannsomware victims to recover their data if the QNAP block-based snapshot feature as described HERE.

While originally named QNAP-NAS-Encrypt, Anomali named it eCh0raix ransomware after a string found within the malware's source code.

The researchers observed that even though the command and control server is located on Tor, the ransomware does not contain any Tor client to connect to it. Instead the ransomware developers created a SOCKS5 proxy that the ransomware connects to inorder to communicate with the C2.

When connecting the C2 server, the ransomware will download the ransom note, a RSA public key used to encrypt the key it employs when encrypting its victims' files, and to provide the attackers with real-time insight on the malware's activity. However, while monitoring this network activity there was no system information sent to the operators to allow them to differentiate between the eCh0raix's victims.

Furthermore, the ransomware developers appear to have created an API that can be used to query for various information. For example, Anomali observed the ransomware connecting to the following URL to retrieve a public encryption key based on a campaign ID. It is not known if these IDs are associated with the ransomware developers personal campaigns or affiliates.

"One of the samples analyzed used the URL "http://sg3dwqfpnr4sl5hh[.]onion/api/GetAvailKeysByCampId/10", that possibly suggests this was the 10th campaign run by the threat actor. "

Encrypting victim's files

When executed on the NAS, the eCh0raix ransomware will perform language checks to see if the device is from certain CIS countries. If so, the ransomware will not encrypt any files.

"The sample found on C2, checks the locale of the infected NAS for Belarus, Ukraine, or Russia and exits without doing anything if a match is found," according to the researchers. "This technique is common amongst threat actors, particularly when they do not wish to infect users in their home country."

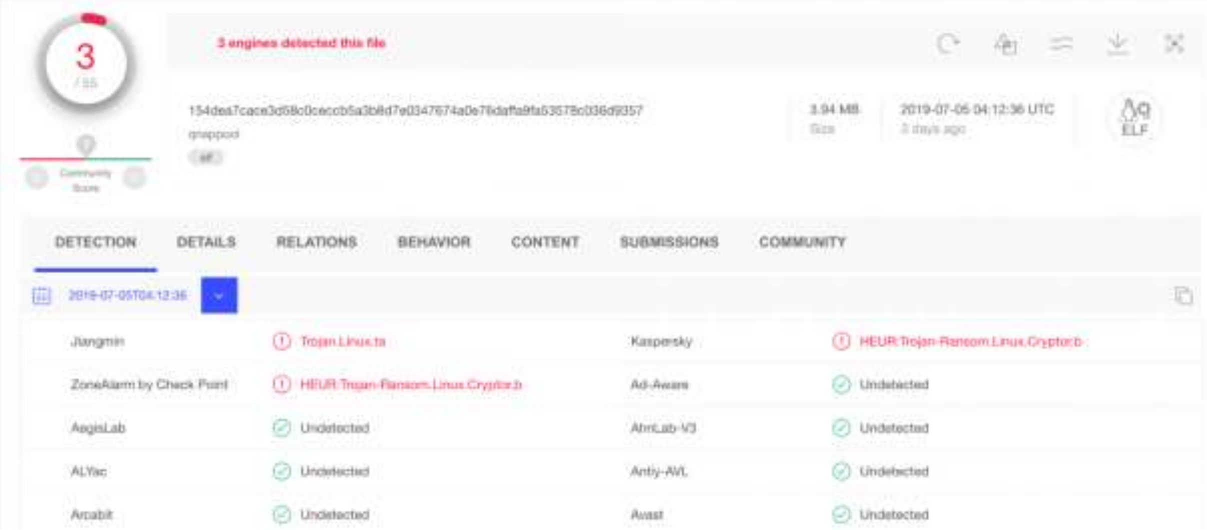
The ransomware will then search for and kill the following process on infected NAS devices using service stop %s or systemctl stop %s commands:

```
apache2
httpd
nginx
mysqld
mysqd
php-fpm
```

eCh0raix will also automatically skip files from file paths that include the following strings when searching for files to encrypt on compromised QNAP devices:

```
/proc
/boot/
/sys/
/run/
/dev/
/etc/
/home/httpd
/mnt/ext/opt
.system/thumbnail
.system/opt
.config
.qpkg.
```

As most QNAP NAS devices do not come with an active anti-malware solution, eCh0raix can freely encrypt documents on compromised systems. To make matters even worse, even on devices where an antivirus product is running in the background, the malware will very rarely be detected as proven by the very low VirusTotal detection date, with only three out of 55 malware scanning engines marking it as malicious.



3 / 55

Community Score

3 engines detected this file

154dea7cace3d58c0ceccb5a3b8d7e0347674a0e76daffa9fa53578c036d9357
qnappod
elf

3.94 MB
Size

2019-07-05 04:12:36 UTC
3 days ago

ELF

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

2019-07-05T04:12:36

Jiangmin	Trojan.Linux.ta	Kaspersky	HEUR:Trojan-Ransom.Linux.Cryptor.b
ZoneAlarm by Check Point	HEUR:Trojan-Ransom.Linux.Cryptor.b	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected

Figure 21 VirusTotal detection rate

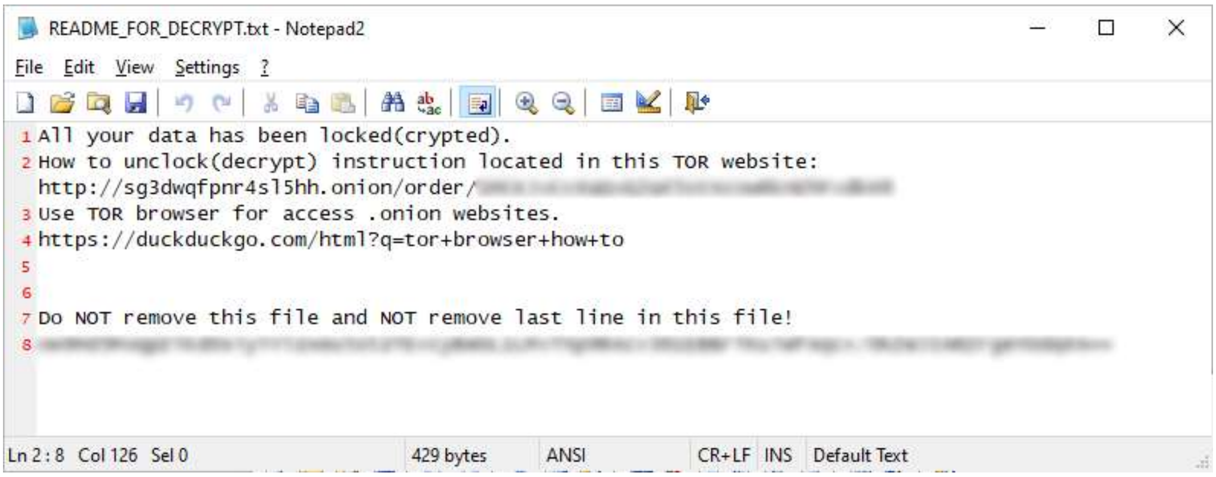
The ransomware is known to encrypt Microsoft Office and OpenOffice documents, PDFs, text files, archives, databases, photos, music, video, and image files using an AES in Cipher Feedback Mode (CFB) secret key created from an AES-256 key generated locally. This AES key is then encrypted with the downloaded or embedded public RSA key and stored in base64 format in the ransom note.

When encrypting files, it will search for the following files types and append the **.encrypted** extension to the encrypted file's name.

```
.dat.db0.dba.dbf.dbm.dbx.dcr.der.dll.dml.dmp.dng.doc.dot.dwg.dwk.dwt.d
xf.dxg.ece.eml.epk.eps.erf.esm.ewp.far.fdb.fit.flv.fmp.fos.fpk.fsh.fwp
.gdb.gho.gif.gne.gpg.gsp.gxk.hdm.hkx.htc.htm.htx.hxs.idc.idx.ifx.iqy.i
so.itl.itm.iwd.iwi.jcz.jpe.jpg.jsp.jss.jst.jvs.jws.kdb.kdc.key.kit.ksd
.lbc.lbf.lrf.ltx.lvl.lzh.m3u.m4a.map.max.mdb.mdf.mef.mht.mjs.mlx.mov.m
oz.mp3.mpd.mpp.mvc.mvr.myo.nba.nbf.ncf.ngc.nod.nrw.nsf.ntl.nv2.nxg.nzb
.oam.odb.odc.odm.odp.ods.odt.ofx.olp.orf.oth.p12.p7b.p7c.pac.pak.pdb.p
dd.pdf.pef.pem.pfx.pgp.php.png.pot.ppj.pps.ppt.prf.pro.psd.psk.psp.pst
.psw.ptw.ptx.pub.qba.qbb.qbo.qbw.qbx.qdf.qfx
```

Figure 22 File types encrypted by eCh0raix

While scanning for files to encrypt, it will also create ransom notes named **README_FOR_DECRYPT.txt** in folders on the NAS. These ransom notes contain a link to a Tor site, an associated bitcoin address, and the users encrypted private encryption key.

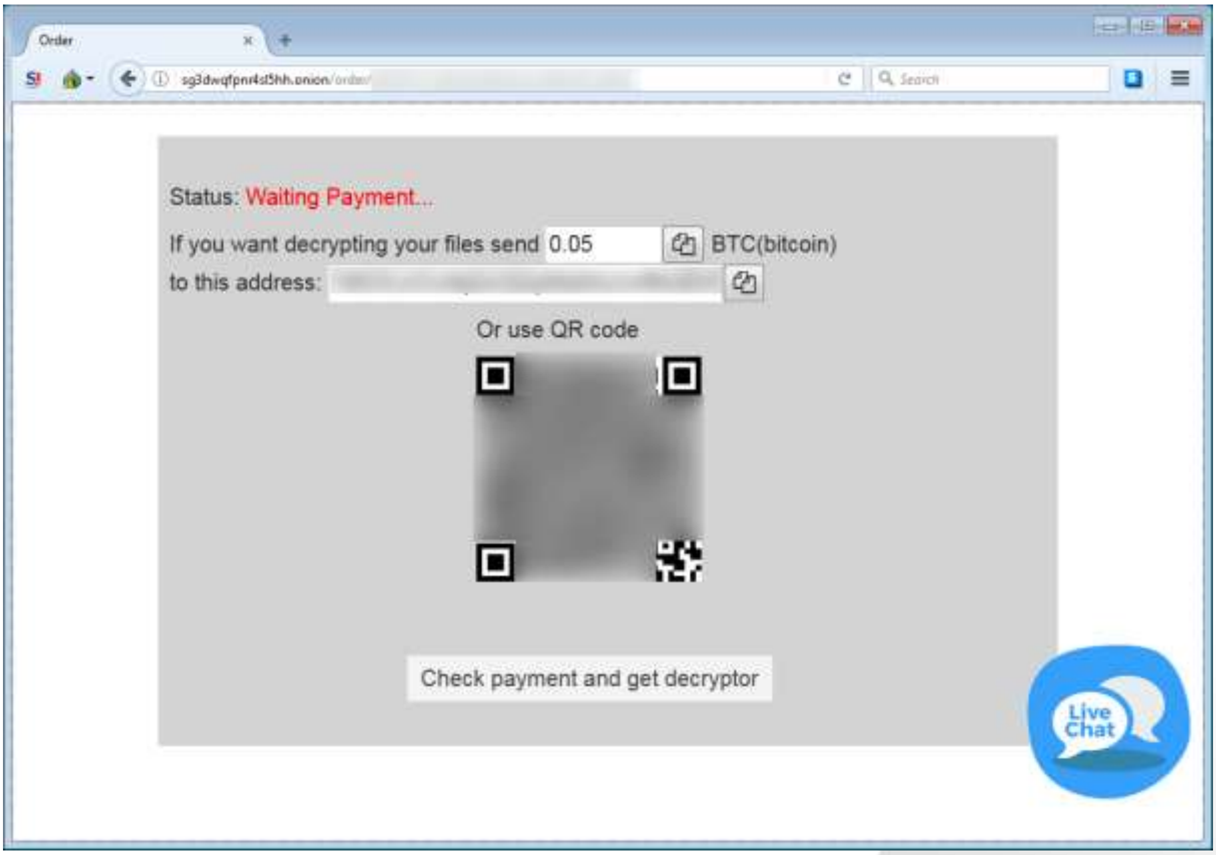


```
All your data has been locked(crypted).
How to unclock(decrypt) instruction located in this TOR website:
http://sg3dwqfpnr4s15hh.onion/order/[redacted]
Use TOR browser for access .onion websites.
https://duckduckgo.com/html?q=tor+browser+how+to


Do NOT remove this file and NOT remove last line in this file!
[redacted]
```

Figure 23 eCh0raix ransom note

If a user goes to the Tor payment site, they will be shown a bitcoin address and the ransom amount that must be sent. The Tor site will allegedly wait for the payment to go through and notify you when it has been received so that you can download the decryptor. In searches by BleepingComputer, the decryptors from the malware developers appear to be available for both Windows and macOS.



Order
sg3dwqfpnr4sl5hh.onion/order/[redacted]
Search

Status: Waiting Payment...

If you want decrypting your files send 0.05 BTC(bitcoin)

to this address: [redacted]

Or use QR code

Check payment and get decryptor
Live Chat

Figure 24 TOR ransomware site with live chat support

According to ransomware researcher Amigo-A, the attackers are asking for "a ransom of 0.05-0.06 BTC or more to return the files".

Decryptor not available yet

While an eCh0raix decryptor is not yet available, the Anomali Threat Research Team says that "Since it is using the math's package to generate the secret key, it is not cryptographically random and it is likely possible to write a decryptor."

Researchers will be taking a look at this ransomware to see if it can be decrypted for free. It is advised that you do not pay the ransom or pay for recovery services until the ransomware has been adequately researched.

Source: https://www.bleepingcomputer.com/news/security/new-ech0raix-ransomware-brute-forces-qnap-nas-devices/

13. Cisco ASA and FTD Software TLS and SSL Driver DoS Vulnerability

A vulnerability in the cryptographic driver for Cisco Adaptive Security Appliance Software (ASA) and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reboot unexpectedly.

The vulnerability is due to incomplete input validation of a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) ingress packet header. An attacker could exploit this vulnerability by sending a crafted TLS/SSL packet to an interface on the targeted device. An exploit could allow the attacker to cause the device to reload, which will result in a denial of service (DoS) condition.

Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed and transparent firewall mode and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic. A valid SSL or TLS session is required to exploit this vulnerability.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190710-asa-ftd-dos

Security Impact Rating: High

CVE: CVE-2019-1873

Source: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190710-asa-ftd-dos?vs_f=Cisco%20Security%20Advisory&vs_cat=Security%20Intelligence&vs_type=RSS&vs_p=Cisco%20ASA%20and%20FTD%20Software%20Cryptographic%20TLS%20and%20SSL%20Driver%20Denial%20of%20Service%20Vulnerability&vs_k=1

14. Hacked Hair Straighteners Can Threaten Homes

A lack of a Bluetooth Low Energy (BLE) pairing mechanism leaves the smart IoT devices open to malicious manipulation.

Researchers have found a way to successfully hack connected hair straighteners to turn them on and increase the heating element up to its maximum temperature—causing a serious fire hazard for unsuspecting owners.

Pen Test Partners decided to put the Glamoriser hair straightener through its security paces, given that it has Bluetooth Low Energy (BLE) embedded for connecting to a mobile app. The app allows a user to remotely change the temperature and set a time frame for automatic shut-off of the device.

"For years we've been trying to set fire to 'smart' things by hacking them. We got some charring on the iKettle, but nothing more," said Stuart Kennedy, in a Friday posting. "These [straighteners] seemed like a much better candidate for our pyromaniac intent."

The straighteners have a maximum temperature that comes in above the flashpoint of paper (233C/451F) – so they could definitely set a fire if left in a vulnerable location. And in fact, it's happened before, no hacking required. Kennedy noted that a U.K. fire service quoted that up to 650,000 house fires have been caused by the accessories.

After downloading the app from the Google Play store, researchers reverse-engineered the code and were able to write a Java script for successfully manipulating the device if it's already turned on. However, all of that turned out to be superfluous effort.

"That there is no pairing or bonding established over BLE when connecting a phone, [so] anyone in range with the app can take control of the straighteners," Kennedy said. In other words, there is no security gate whatsoever or individual authentication between the app and the straightener. Through the app, anyone within range of the device can override the settings of the owner – say, increasing the temperature and elongating the automatic shut-off time to its longest duration, which is 20 minutes.

Figure 25 Glamoriser straightener

"Yes, this attack requires the hacker to be within Bluetooth range, but it would have been so easy for the manufacturer to include a pairing/bonding function to prevent this," Kennedy said. "Something as simple as a button to push to put the straighteners in pairing mode would have solved it. Instead, we now have a method to set fire to houses."

He added that while a mitigation to any real-world attack is the fact that only one app can connect to the device at any one time, this obstacle is likely not a large one in most households.

"The straighteners do not support more than one concurrent phone connection, though I can see a lot of people buying the straighteners and never actually getting 'round to connecting a phone to them, so they're exposed," Kennedy said. "Also, if the user goes out of BLE range, your local neighborhood hair straightener hacker can jump in and pump up the temperature."

Average BLE range is around 10 to 20 meters (though it has a theoretical range of up to 100 meters), so any attack would need to come from someone inside the house (a disgruntled younger sibling, perhaps?) or from someone lurking directly outside. If the latter, there are perhaps other dangers to worry about. But the research points out that once again, internet of things (IoT) devices lack security by design.

"Since this is Bluetooth and requires you to be in range to exploit it, the probability of exploration from a hacker is very low, unless you make a sibling or neighbor (if you live in an apartment) mad at you," said Lamar Bailey, senior director of security research at Tripwire, via email. "If you have this device, remember to be nice to anyone who could be within 33 feet of you straightening your hair."

Those devices that use BLE, which is custom-made for low-power IoT sensor applications, is of particular concern, given that unlike the full implementation of the Bluetooth spec, BLE doesn't require authentication in order to pair devices. Thus, many device-makers fail to take the extra step to build it in.

"Authentication depends entirely on the developers of the device, and experience shows that it is often neglected," researchers Roman Unuchek and Roland Sako said in a posting last year outlining research on pet trackers last year. In that analysis BLE was found to connect these pet-trackers to the owner's smartphone, but were left wide open to man-in-the-middle attacks.

Source: https://threatpost.com/firestarter-hacked-hair-straighteners/146434/

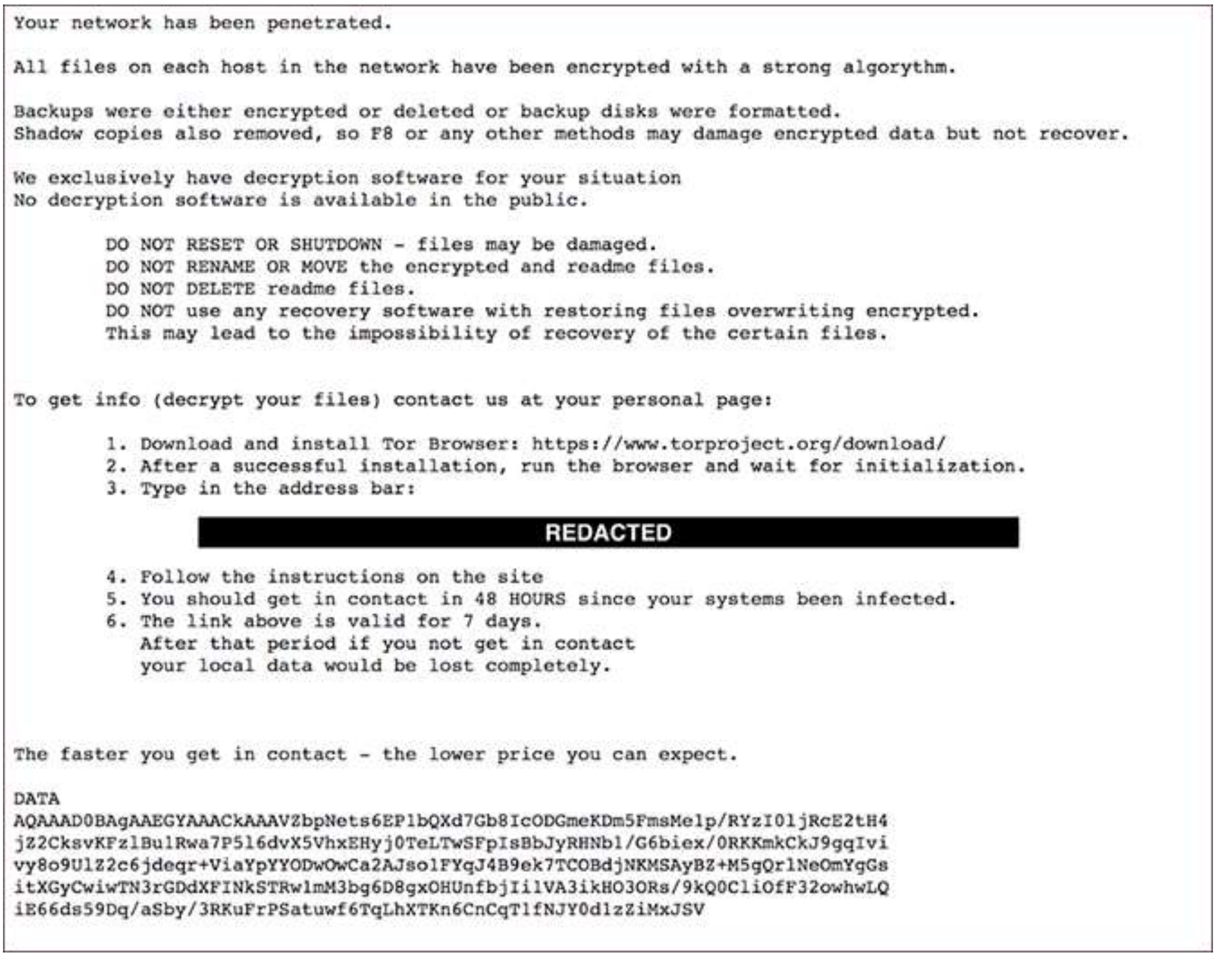
15. New DoppelPaymer Ransomware Emerges from BitPaymer's Code

Malware researchers have discovered a new file-encrypting malware they dubbed DoppelPaymer that has been making victims since at least mid-June, asking hundreds of thousands of US dollars in ransom.

The ransomware strain has at least eight variants that extended their feature set gradually, with the earliest one dating since April.

Victims in the public service sector

DoppelPaymer takes its name from BitPaymer, with which it shares more than large portions of code. There are three confirmed victims of this ransomware strain, which priced its decryption keys between 2 BTC and 100 BTC, say researchers from CrowdStrike.



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: https://www.torproject.org/download/
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

                                REDACTED

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 7 days.
           After that period if you not get in contact
           your local data would be lost completely.


The faster you get in contact - the lower price you can expect.

DATA
AQAAAD0BAgAAEGYAAACkAAAVZbpNets6EP1bQXd7Gb8IcODGmeKDm5FmsMe1p/RYzI01jRcE2tH4
jZ2CksvKFzlBulRwa7P5l6dvX5VhxEHyj0TeLTwSFpIsBbJyRHNbl/G6biex/0RKKmkCkJ9gqIvi
vy8o9UlZ2c6jdeqr+ViaYpYYODwOwCa2AJsolFYqJ4B9ek7TCOBdjNKMSAyBZ+M5gQrlNeOmYgGs
itXGyCwiwTN3rGDdXFINkSTRwlmM3bg6D8gxOHUnfbjIilVA3ikHO3ORs/9kQ0CliOfF32owhwLQ
iE66ds59Dq/aSby/3RKuFrPSatuwf6TqLhXTKn6CnCqTlfNJY0dlzZiMxJSV
```

Figure 26 DoppelPaymer Ransom Note

Bitcoin price in late April was around $5,150 and kept rising ever since, with lows well above the $7,000 mark and peaking above $12,000 in late June and early July.

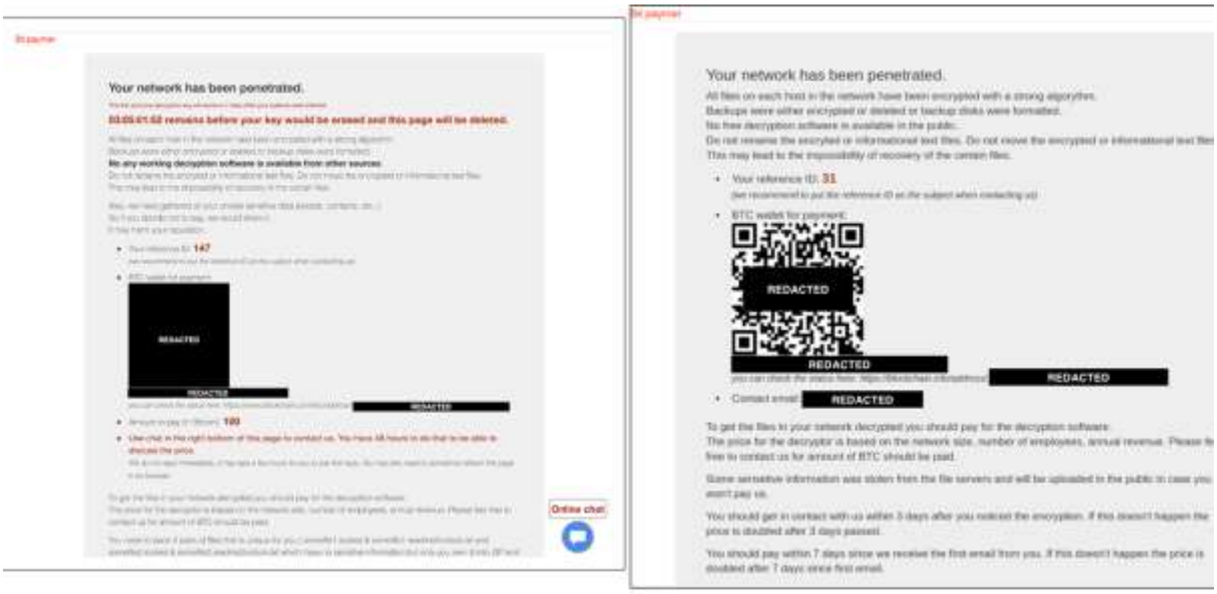
One of the victims is the City of Edcouch, Texas, which was left with a ransom note demanding 8 BTC to decrypt the data on the affected computers.

It is unclear when the Edcouch administration was attacked, but city officials said that the amount converted to about $40,000. This makes it likely that the compromise happened in early May or before when bitcoin price stooped below $5,500.

Another victim was the Chilean Ministry of Agriculture, the researchers said in a report last week. The country's Computer Security Incident Response Team (CSIRT) confirmed on July 1 that a ransomware attack hit servers from a public service connected to the Ministry of Agriculture.

Parallel extortion activity

CrowdStrike researchers observed some striking similarities between DoppelPaymer's payment portal and the original one for BitPaymer. One striking hint linking the two ransomware threats is the "Bit paymer" title at the top of the page but they're similar all over.



Your network has been penetrated.

[illegible]

03:05:01:52 remains before your key would be erased and this page will be deleted.

[illegible]
No any working decryption software is available from other sources.
[illegible]

[illegible]

- [illegible] 147
- [illegible]
  REDACTED
  REDACTED
  [illegible] REDACTED
- [illegible] 100
- Use chat in the right bottom of this page to contact us. You have 48 hours to do that to be able to discuss the price.
  [illegible]

[illegible]

Online chat

DoppelPaymer payment portal

Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorythm.
Backups were either encrypted or deleted or backup disks were formatted.
No free decryption software is available in the public.
Do not rename the encryted or informational text files. Do not move the encrypted or informational text file
This may lead to the impossibility of recovery of the certain files.

- Your reference ID: 31
  (we recommend to put the reference ID as the subject when contacting us)
- BTC wallet for payment:
  REDACTED
  REDACTED
  you can check the status here: https://blockchain.info/address/ REDACTED
- Contact email: REDACTED

To get the files in your network decrypted you should pay for the decryption software.
The price for the decryptor is based on the network size, number of employees, annual revenue. Please fe
free to contact us for amount of BTC should be paid.

Some sensitive information was stolen from the file servers and will be uploaded in the public in case you
won't pay us.

You should get in contact with us within 3 days after you noticed the encryption. If this doesn't happen the
price is doubled after 3 days passed.

You should pay within 7 days since we receive the first email from you. If this doesn't happen the price is
doubled after 7 days since first email.

Older BitPaymer payment portal

Figure 27 DoppelPaymer/BitPaymer Payment Portals

Another clue pointing to a connection between the two pieces of malware is that they "share significant amounts of code." However, they have different encryption schemes.

Where DoppelPaymer combines 2048-bit RSA keys with 256-bit AES, the latest BitPaymer versions use 4096-bit RSA with the same specification for symmetric encryption.

Also, there is standard AES encryption padding (PKCS#7) in DoppelPaymer while BitPaymer uses random bytes specified in a field called 'TAIL.'

By analyzing differences and similarities between the two, Brett Stone-Gross, Sergei Frankoff and Bex Hartley of CrowdStrike's research and threat intel team believe that the new ransomware strain may be the work of a BitPaymer group member that started their own ransomware business.

> "Both BitPaymer and DoppelPaymer continue to be operated in parallel and new victims of both ransomware families have been identified in June and July 2019. The parallel operations, coupled with the significant code overlap between BitPaymer and DoppelPaymer, indicate not only a fork of the BitPaymer code base, but an entirely separate operation." - CrowdStrike

The new ransomware includes modifications that make it superior to BitPaymer, such as threaded encryption process for a quicker operation.

The operators of BitPaymer are the same individuals behind the Dridex banking trojan, collectively known as the INDRIK SPIDER. They are former affiliates of the cybercriminal gang calling itself "The Business Club."

The group is responsible for using the GameOver Zeus botnet (disrupted in 2014), believed to have infected over one million computers, and causing damages in excess of $100 million from business and financial institutions across the world.

Source: https://www.bleepingcomputer.com/news/security/new-doppelpaymer-ransomware-emerges-from-bitpaymers-code/

16. Turla APT Returns with New Malware, Anti-Censorship Angle

A dropper called "Topinambour" is the first-stage implant, which in turn fetches a spy trojan built in several coding languages.

The Turla APT has revamped its arsenal in 2019, creating new weapons and tools for targeting government entities. It's now using booby-trapped anti-internet censorship software as an initial infection vector, suggesting Turla is going after dissident or other civil-society targets.

The Russian-speaking actors believed behind Turla named the dropper "Topinambour," which is another word for the Jerusalem artichoke (a.k.a. the sunchoke). Since January, Topinambour has become the first-stage implantation for Turla campaigns. Once installed, it fetches all the other malware that the group uses to gain access to target networks and exfiltrate information.

"To deliver [the new modules] to targets, the operators use legitimate software installers infected with the Topinambour dropper," researchers at Kaspersky wrote in a malware analysis on Monday. "These could be tools to circumvent internet censorship, such as Softether VPN 4.12 and psiphon3, or Microsoft Office activators." The latter are exceptions to the anti-censorship ploys and are used by software pirates to activate the Microsoft Office suite without having to buy the actual product key.

The abuse of installation packs for VPN software, which can bypass internet censorship, suggests the attackers have clearly defined cyberespionage targets for these tools, the firm added.

Russian-speaking Turla (a.k.a. Snake, Venomous Bear, Waterbug and Uroboros) is known for spy campaigns targeting Western governments as well as embassies and consulates in post-Soviet states. It's been active since at least 2014 (and possibly earlier) developing a range of custom backdoors to carry out its work. It continually evolves both in terms of malware and targets.

Latest Toolset

The Topinambour dropper contains what Kaspersky calls a "tiny .NET shell" that will wait for Windows shell commands from the command-and-control server (C2) and silently execute them. The C2 infrastructure is hosted on compromised WordPress sites and on cloud services.

“Using this and SMB shares on rented virtual private servers (VPS) [in South Africa], the campaign operators spread the next-stage modules using just ‘net use’ and ‘copy’ Windows shell commands,” the researchers noted.

One of these next-stage modules is an already-known Turla tool, the KopiLuwak JavaScript trojan, but more interestingly, Turla has crafted heavily obfuscated PowerShell and .NET trojans that are similar to KopiLuwak, the analysis found. Both (dubbed MiamiBeach and RocketMan!, respectively) were used in an active campaign that started at the beginning of 2019.

The researchers hypothesize that one of the reasons for creating similar trojans in different languages could be to avoid detection. “If one version is detected on the victim’s computer, the operators can try an analogue in a different language,” they explained. “The reason behind the development of KopiLuwak’s PowerShell and .NET analogues may be simply to minimize detection of the well-known, publicly discussed JavaScript versions.”

The trojans upload, download and execute files, and fingerprint target systems. The PowerShell version of the trojan also has the ability to capture screenshots. They communicate with the C2 from an opened SMB share on a remote CELL-C VPS in South Africa.

And, they also retrieve a final-stage, more complex trojan, able to parse and execute custom commands from the C2, the researchers added. During the final stage of infection, this encrypted trojan for remote administration is embedded into the computer’s registry for the malware to access when complete.

“The purpose of all this infrastructure and modules in JavaScript, .NET and PowerShell is to build a fileless module chain on the victim’s computer consisting of an initial small runner and several Windows system registry values containing the encrypted remote administration tool,” the researchers wrote. “Using the Windows system registry to store encrypted data that is later used by the malware also seems to be aimed at minimizing detection and reducing the digital footprint on any victim’s computer, where only a tiny starter would be left.”

Source: https://threatpost.com/turla-apt-malware-anti-censorship/146472/

17. BEC Scams Average $301 Million Per Month In Illegal Transfers

The frequency of business email compromise (BEC) scams has increased year over year and so did the value of attempted thefts, reaching a monthly average of more than $300 million.

The number is drawn from the suspicious activity reports (SARs) received every month since 2016, which increased from 500 to more than 1,100 in 2018.

The Financial Crimes Enforcement Network (FinCEN) compiled statistics about BEC incidents occurring over the past two years and identified the most common types of targets along with the destination intended for the stolen funds and the techniques used by the scammers.

The latest report from Internet Crime Report from FBI's Internet Crime Complaint Center (IC3) informs BEC scams were responsible for most of the losses generated by cybercrime.

Companies lost $1.2 billion to this sort of cybercriminal activity that aims to obtain funds by posing as a customer or upper management personnel in a company in order to trick key individuals in the organization into wiring funds to an attacker-control bank account.

Statistics are dire

FinCEN's analysis describes the broader picture of BEC scams stating that while scammers tried to steal in 2016 an average of $110 million per month the value in 2018 grew to $301 million.

According to these numbers, last year alone cybercriminals endeavored to rob companies of more than $3.6 billion.

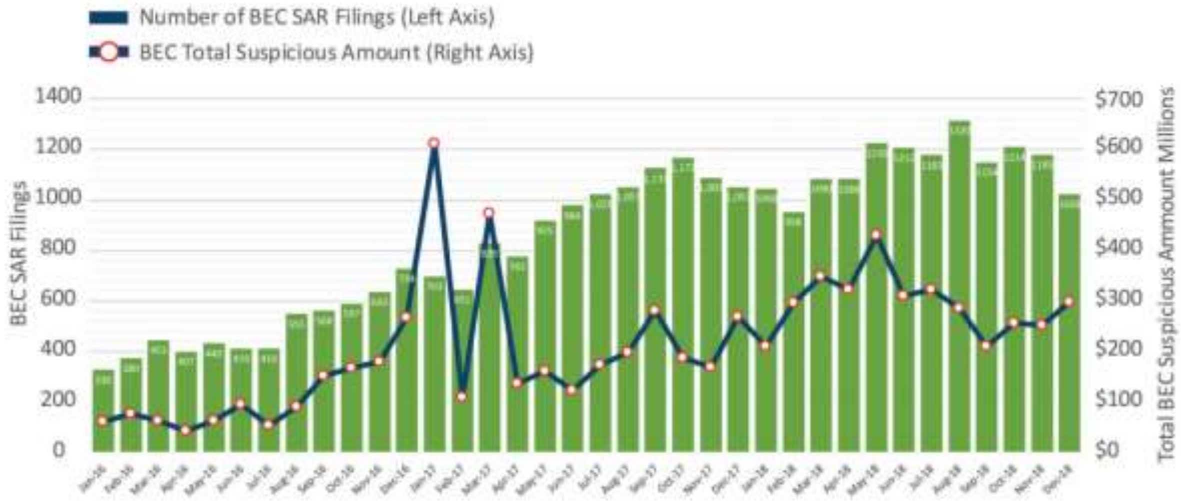


Figure 28 Monthly BEC SAR Filings and Total Suspicious Transaction Amount

"In 2016, financial institutions filed nearly 6,000 BEC-related SARs with an average transaction total of $110 million per month. In 2017, the number of BEC-related SARs increased to over 11,000 with a monthly average of $241 million. In 2018, the number of BEC-related SARs rose to nearly 14,000 filings, averaging $301 million in suspicious transactions per month" - FinCEN

Most common victims

The organization's assessment shows that companies in the manufacturing or construction business were the most frequent targets of email account compromise attacks, accounting for 25% of the victims.

Commercial entities offering professional services like landscaping, retail, restaurants, and lodging became more attractive targets, with 18% of the attacks being aimed at them.

Unlike financial organizations, which fell in the rankings from 16% to 9%, real estate firms turned out to be more tempting, representing 16% of the BEC scam victim pie.

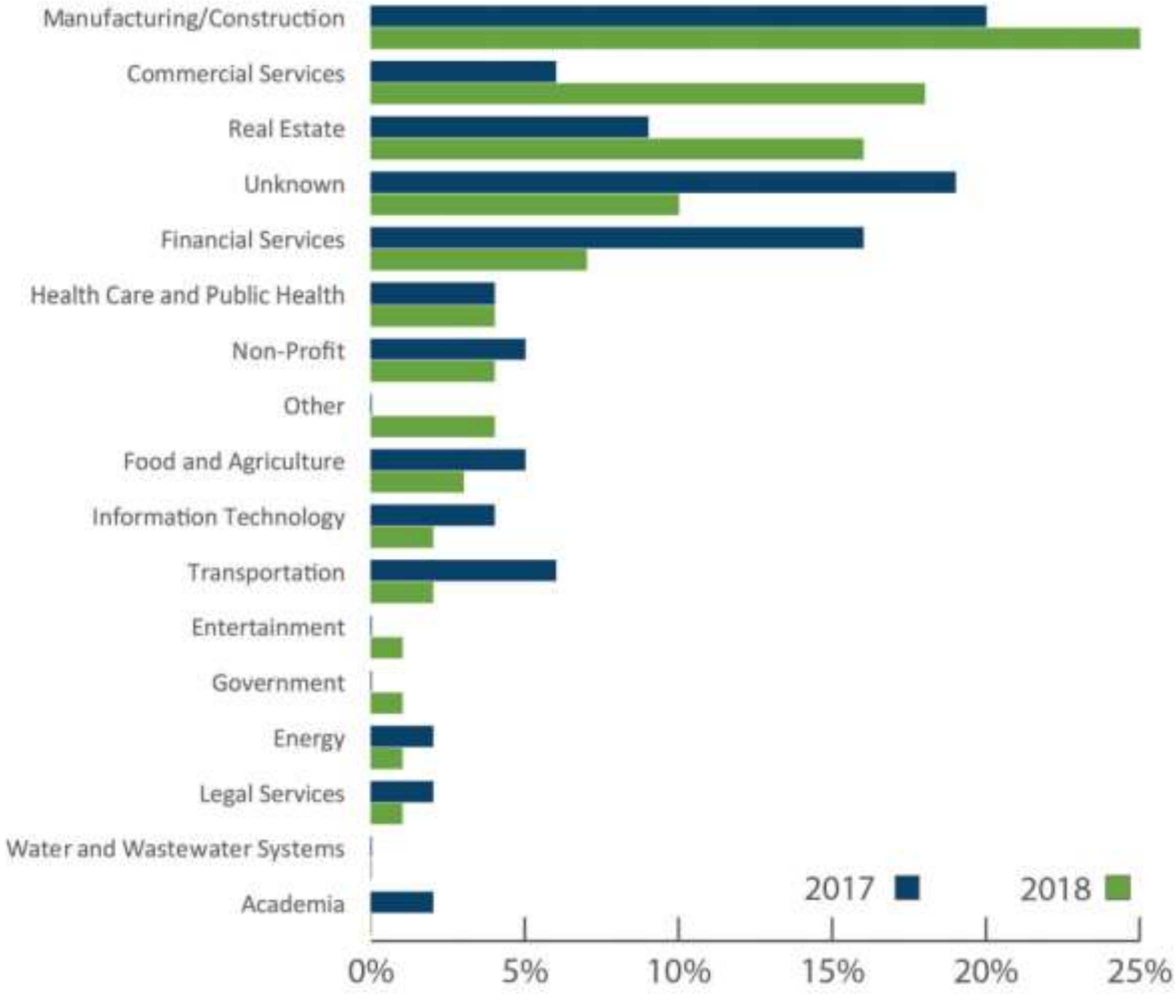


Figure 29 2017 and 2018 BEC Targets by Industry

Most of the wire transfers from BEC fraud are domestic, FinCEN observed. In 73% of the cases the beneficiary is in the U.S. and only 27% of the transactions have a foreign destination.

This does not mean that the majority of the threat actors are US-based. These figures likely reflect the fact that cybercriminals use money mules to withdraw the money, which is later distributed across the cybercriminal network and typically ends up abroad.

Top BEC methods

Crooks have different tactics to attain their goal. In 2017 they used to impersonate company CEOs, which have sufficient authority to instruct individuals in charge of making payments to wire money to a specific account.

This approach dropped from 33% to 12% in 2018, indicating that fraudsters are adapting and looking for new ways to play their tricks.

Last year they seemed to prefer impersonating customers and vendors, and used fake invoices in an attempt to get paid. They are also adjusting the sums according to the industry sector tackled.

"The average transaction amount for BECs impersonating a vendor or client invoice was $125,439, compared with $50,373 for impersonating a CEO" - FinCEN

One example in the report is of a Lithuanian man who used fake invoices to defraud multinational companies of at least $100 million; the money was wired to overseas accounts he controlled.

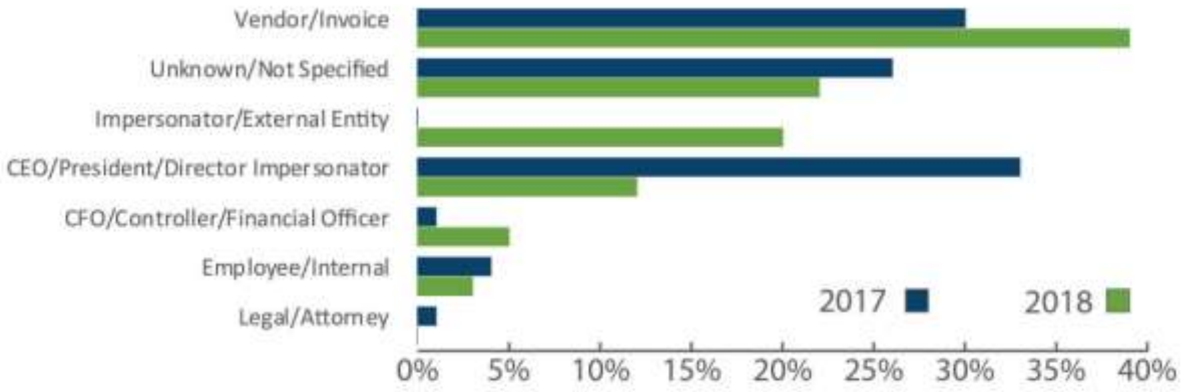


Figure 30 2017 and 2018 BEC Identified Scam Types

Although the instructions for transferring the money are done over email, scammers need to prepare the message so that it does not raise any suspicions.

For this, they rely on various malware designed to steal the necessary info for perpetrating the attack. Spyware is the common threat as it steals the data necessary to break into email accounts.

However, the trend seems to change. Nigerian fraudsters, who are skilled in the scamming business, started to shift to remote access tools that provide a higher set of capabilities.

Source: *https://www.bleepingcomputer.com/news/security/bec-scams-average-301-million-per-month-in-illegal-transfers/*

18. Facebook to Pay Over $5 Billion Following FTC, SEC Settlements

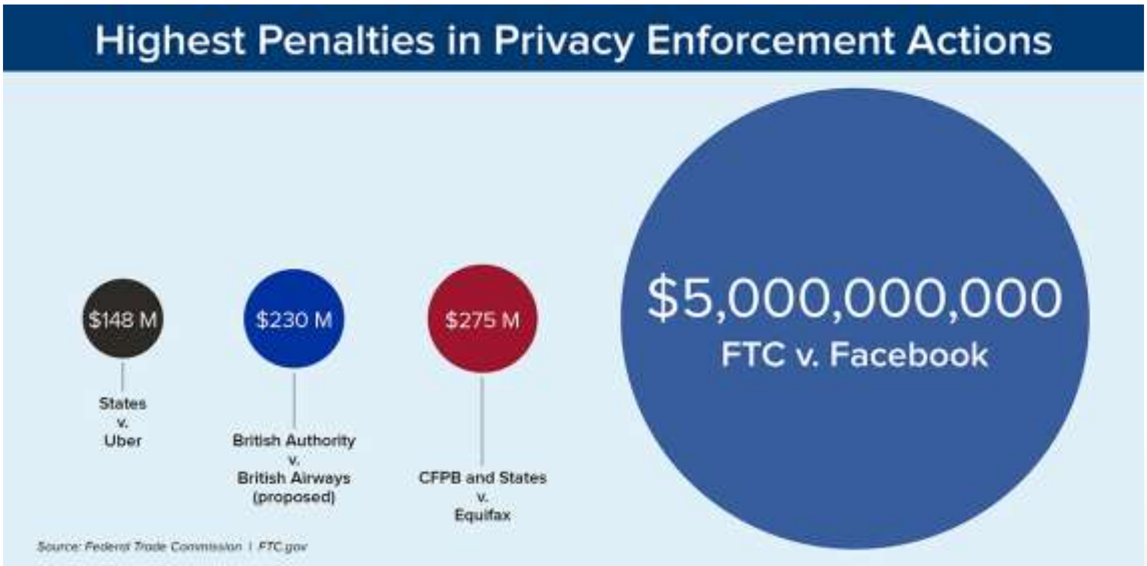
An agreement with the Federal Trade Commission (FTC) requires Facebook to pay a $5 billion penalty, to implement a new privacy and information protection framework, and to provide the FTC with new monitoring tools after an investigation launched following the Cambridge Analytica events.

The settlement is designed to resolve charges alleging that the company violated an FTC consent order from 2012 "by deceiving users about their ability to control the privacy of their personal information."

This is the largest ever consumer privacy violation penalty paid by a company and among the largest ones ever imposed by the U.S. Government for any type of violation.

"Despite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers’ choices," stated FTC Chairman Joe Simons. “The magnitude of the $5 billion penalty and sweeping conduct relief are unprecedented in the history of the FTC."

"The relief is designed not only to punish future violations but, more importantly, to change Facebook’s entire privacy culture to decrease the likelihood of continued violations. The Commission takes consumer privacy seriously, and will enforce FTC orders to the fullest extent of the law."



Source: Federal Trade Commission | FTC.gov

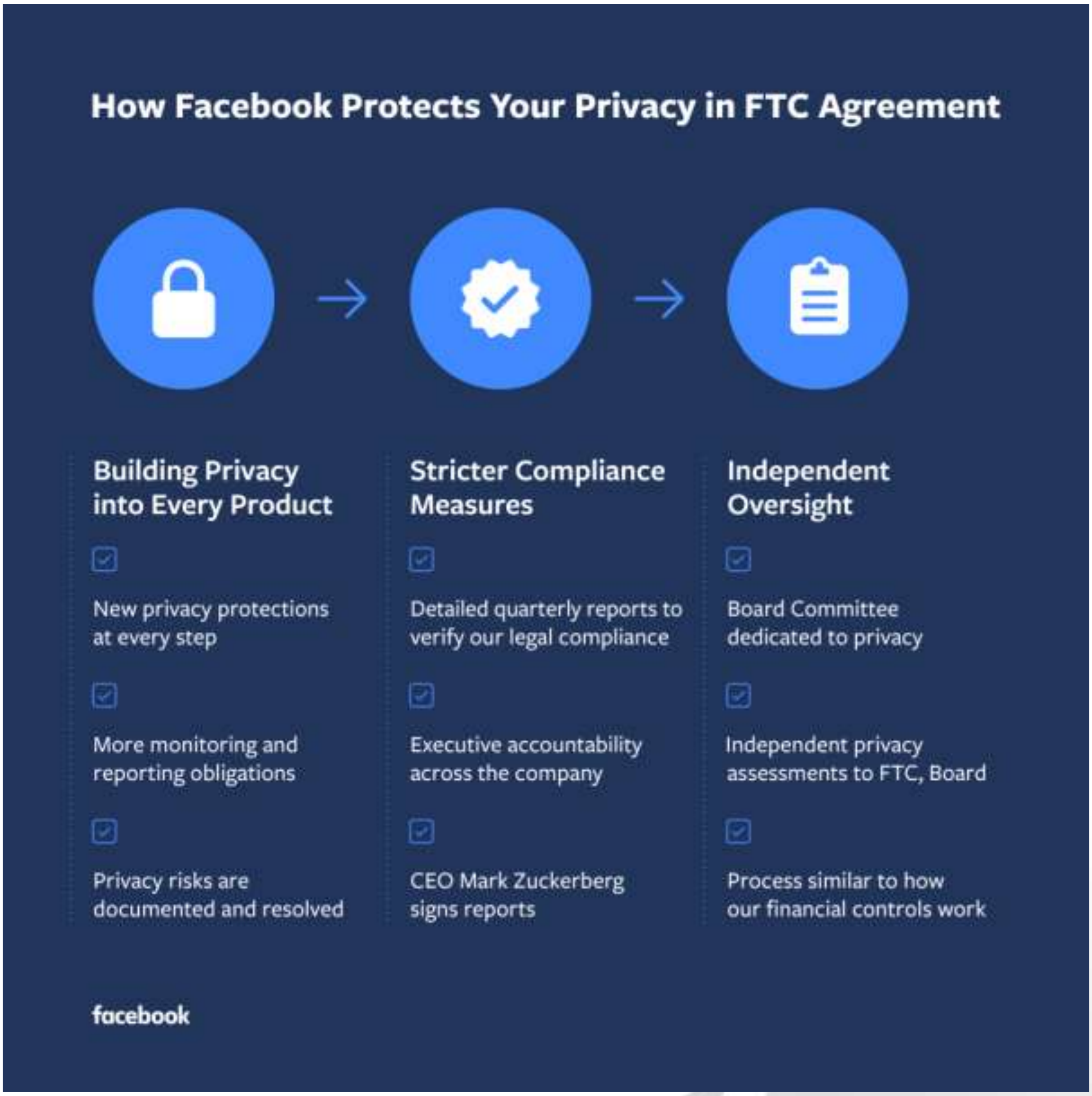
Figure 31 Highest Penalties in Privacy Enforcement Actions

Facebook is also required under the settlement's terms to build a multilayered compliance system comprised of an independent privacy committee, compliance officers, and a third-party assessor working in conjunction with the CEO to prevent future events where users are deceived about privacy measures.

Quarterly certifications will be submitted by the compliance officers and Facebook's CEO to the FTC to show that the company is still complying with the privacy framework imposed by the new FTC order.

The independent third-party assessor will detect any gaps in the company's order-mandated privacy program [PDF] which it will directly report on a quarterly basis to the new privacy committee, independent of Facebook's board of directors, with members removable only by a board supermajority.

Facebook also has to "conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy" per the privacy order.



How Facebook Protects Your Privacy in FTC Agreement

Building Privacy into Every Product

☑ New privacy protections at every step

☑ More monitoring and reporting obligations

☑ Privacy risks are documented and resolved

Stricter Compliance Measures

☑ Detailed quarterly reports to verify our legal compliance

☑ Executive accountability across the company

☑ CEO Mark Zuckerberg signs reports

Independent Oversight

☑ Board Committee dedicated to privacy

☑ Independent privacy assessments to FTC, Board

☑ Process similar to how our financial controls work

facebook

Figure 32 Facebook's steps in protecting the user's privacy in FTC Agreement

The company will also have to document, record, and share all events impacting the data of more than 500 users with the new privacy commission and the independent assessor within 30 days after the incident was discovered.

Supplementary privacy obligations also require that:

- Facebook must exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data;
- Facebook is prohibited from using telephone numbers obtained to enable a security feature (e.g., two-factor authentication) for advertising;
- Facebook must provide clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users;
- Facebook must establish, implement, and maintain a comprehensive data security program;
- Facebook must encrypt user passwords and regularly scan to detect whether any passwords are stored in plaintext; and
- Facebook is prohibited from asking for email passwords to other services when consumers sign up for its services.

"The agreement will require a fundamental shift in the way we approach our work and it will place additional responsibility on people building our products at every level of the company," said Facebook in a blog post. "It will mark a sharper turn toward privacy, on a different scale than anything we've done in the past."

Also, as detailed by Ime Archibong, Facebook's VP of Product Partnerships, the company also terminated access to collected user data for two of its partners, Microsoft and Sony, which were still using "old code supporting known experiences for people, such as being able to use Facebook on an earlier generation PlayStation (PS3 or Vita) or to sync their friends' contact information with another service."

"Based on our previous commitments, we are ending these partners' access to friend data immediately. This was our mistake, and we are correcting it," added Archibong.

$100 million SEC settlement

Another settlement was agreed upon with the Securities and Exchange Commission (SEC) to resolve an investigation on Facebook's failure to include more info regarding the Cambridge Analytica incident with its investor disclosures.

As part of this second settlement with the SEC, Facebook will have to pay an extra $100 million penalty "for making misleading disclosures regarding the risk of misuse of Facebook user data", on top of the $5 billion it agreed to pay to the Treasurer of the United States as part of the FTC settlement.

“We allege that Facebook exacerbated its disclosure failures when it misled reporters who asked the company about its investigation into Cambridge Analytica,” said Erin E. Schneider, Director of the SEC’s San Francisco Regional Office. “This gave further weight to Facebook’s misleading statements in its public filings.”

Source: [*https://www.bleepingcomputer.com/news/technology/facebook-to-pay-over-5-billion-following-ftc-sec-settlements/*](https://www.bleepingcomputer.com/news/technology/facebook-to-pay-over-5-billion-following-ftc-sec-settlements/)

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

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

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

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