Digital / Cyber Forensic & Compromise Assessment

OBJECTIVES

OBJECTIVES

Workshop Objective

- Understand the need of compromise assessment
- Gain visibility of malicious activity, identify and confirm the breach.
- Develop ability to foresee and assess upcoming cyber challenges
- Collect evidence for an effective response with law enforcement, partners and customers.
- Improve internal capacity for incident detection, containment & mitigation

Introduction to Cyber Forensic
Demonstration of Email Spoofing

Cyber Investigation Against Mobile Devices
Next Gen Cyber Blunders by Experts

Advance Level compromise assessment
Role of an Individual during compromise assessment
Demonstrating a scenario of compromise assessment

Demonstration to find attacks who are currently in the environment or had been active

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Introduction to cyber forensic

INTRODUCTION TO CYBER FORENSIC

Cyber forensics, e-discovery (electronic evidence discovery), digital forensics, computer forensics, all relevant, each meaning relatively the same thing, and depending on whom you speak with, each meaning something very different, yet none has emerged as a de facto standard.

The term specifically used for collecting, examining, Analyzing & reporting of data from the device.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

INTRODUCTION TO COMPROMISE ASSESSMENT

INTRODUCTION TO COMPROMISE ASSESSMENT

Compromise assessment is a proactive approach for evaluation of systems to detect threat that have evaded existing controls.

A compromise can be defined in three states:

- **Applications** – Applications become one of the weakest link in compromise the systems, lack of application level security controls may lead towards compromise. For e.g.(SQL, Apache, IIS, torrent, WinRAR, Acrobat) etc.

- **Operating System** – Operating systems are another way of compromising the accessibility of the system by triggering up a OS level vulnerability. For e.g. (Windows, Linux, Solaris) etc.

- **Network** – Networks connects applications and operating system by means of IP addresses and ports numbers. Network side become vulnerable if not properly organized by a known professional which may leads towards compromise state. Network attacks which may leads towards compromise are included but not limited to ARP Spoofing, DNS Spoofing, IP Flooding, IP Spoofing, DHCP Starvation) etc.

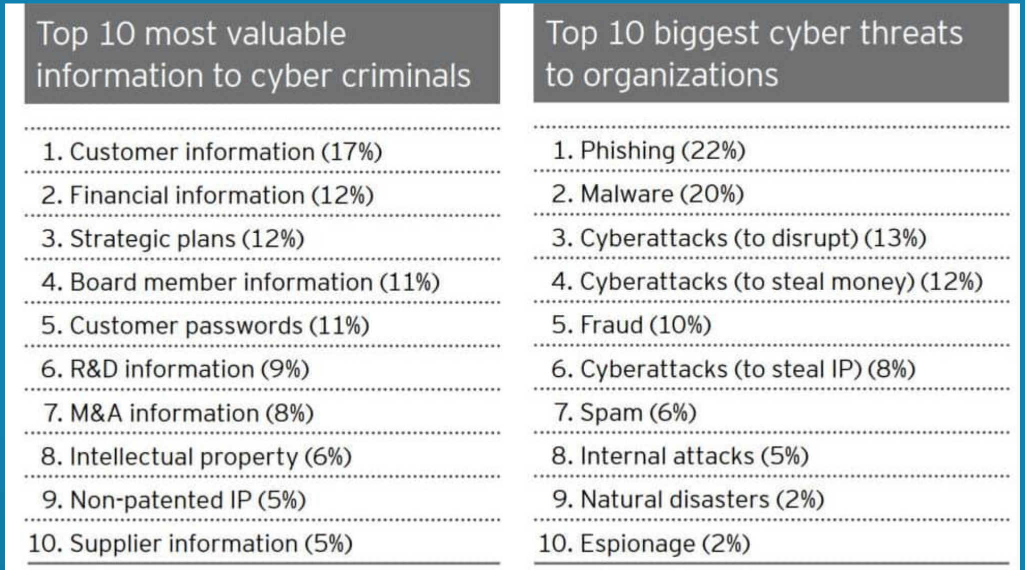
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Email Spoofing

EMAIL SPOOFING

Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open and reply to the email seems urgent in by its content and requires some financial or confidential data from the user.

According to the survey conducted by E&Y the statistics shows that 22% of the attacks comes by running a phishing campaign against the organization.



Top 10 most valuable information to cyber criminals	Top 10 biggest cyber threats to organizations
1. Customer information (17%)	1. Phishing (22%)
2. Financial information (12%)	2. Malware (20%)
3. Strategic plans (12%)	3. Cyberattacks (to disrupt) (13%)
4. Board member information (11%)	4. Cyberattacks (to steal money) (12%)
5. Customer passwords (11%)	5. Fraud (10%)
6. R&D information (9%)	6. Cyberattacks (to steal IP) (8%)
7. M&A information (8%)	7. Spam (6%)
8. Intellectual property (6%)	8. Internal attacks (5%)
9. Non-patented IP (5%)	9. Natural disasters (2%)
10. Supplier information (5%)	10. Espionage (2%)

Reference.: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

EMAIL SPOOFING(CONT'D)...

Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open and reply to the email seems urgent in by its content and requires some financial or confidential data from the user.

DEMONSTRATION

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

EMAIL SPOOFING – PREVENTION

EMAIL SPOOFING PREVENTION

A spoofed email message is modified to appear as if it originates from a sender other than the actual sender of the message. To stop email spoofing, following are the key step which requires special considering when securing from email spoofing.

Using Sender ID to counter from spoofing attack;
Creating **Sender Policy Framework (SPF)** record entry: Sender Policy Framework – or SPF as it is commonly known – is a solution created in an attempt to validate the source of an email message received by a mail system.
SPF policies work by adding a TXT record to your email domain's DNS (domain name server) that identifies the authorized mail servers for sending email for this domain

An example record:
v=spf1 include:mail.example.com -all

Reference.: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

EMAIL SPOOFING PREVENTION (CONT’D)…

A spoofed email message is modified to appear as if it originates from a sender other than the actual sender of the message. To stop email spoofing, following are the key step which requires special considering when securing from email spoofing.

Configuring **Domain Message Authentication Reporting and Conformance (DMARK)** record - DMARC not only advises the receipt to quarantine or reject the email message on failure, but also asks for a report of the message to be sent to a reporting address. This is a great step for gaining some insight into spam/malspam campaigns spoofing your organization.

An example record:
V=DMARC1; p=none; rua=mailto:report.rua@example.com;
ruf=mailto:report.ruf@example.com;

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

EMAIL SPOOFING PREVENTION (CONT'D)...

A spoofed email message is modified to appear as if it originates from a sender other than the actual sender of the message. To stop email spoofing, following are the key step which requires special considering when securing from email spoofing.

Domain Keys Identified Mail (DKIM) - DKIM this is used to publish the signer's public key, which the recipient mail server then uses to verify that the content signed by the digital signature is included in the email message headers.

An example DKIM record:
V=DKIM1; k=rsa; p=PUBLICKEY

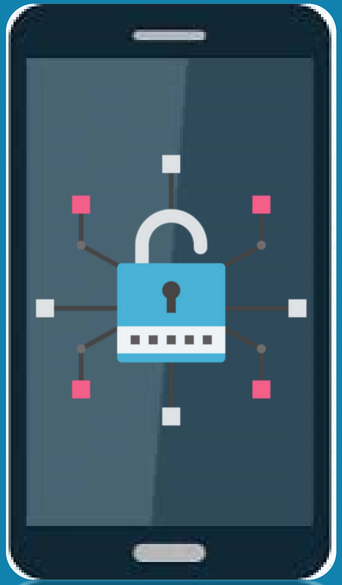
Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Cyber Investigations Against Mobile Devices

CYBER INVESTIGATION AGAINST MOBILE DEVICES

Mobile device is become one of key threat which user is are carrying with them. Its not like a hand grenade but it is not less then a hand grenade the difference is that a hand grenade can physically harm and this threat can logically harm user by stealing the privacy of the users data.

Cybercriminals targeting mobile devices most frequently use apps to break in, as seen in **79%** of mobile-focused attacks in 2019 and **76%** of those in 2020 so far, Pradeo Labs researchers found.

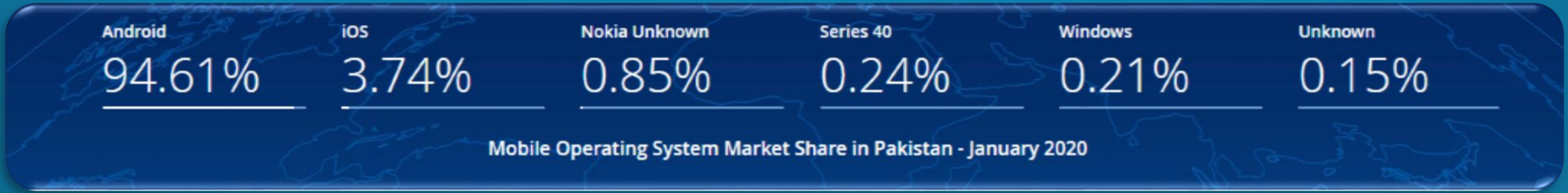


Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

CYBER INVESTIGATION AGAINST MOBILE DEVICES (CONT'D)…

MOBILE PHONE USERS STATISTICS IN PAKSITAN

According to the latest stats of Pakistani market, **94.61%** are using android based cell phone devices, **3.74%** are using iOS devices.



Android 94.61%

iOS 3.74%

Nokia Unknown 0.85%

Series 40 0.24%

Windows 0.21%

Unknown 0.15%

Mobile Operating System Market Share in Pakistan - January 2020

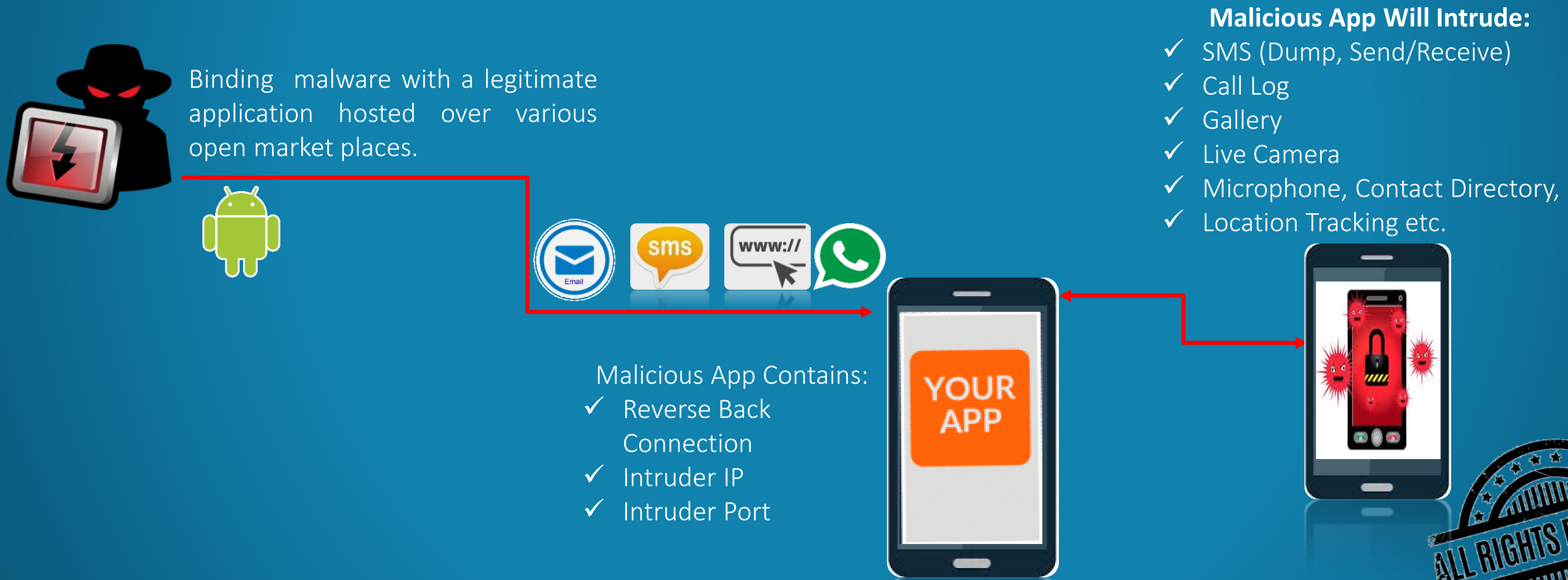
Date	Android	iOS	Nokia Unknown	Series 40	Unknown	Windows	Symbian OS	Samsung	BlackBerry OS	Linux	Other
2019-11	95.21	3.06	0.9	0.27	0.16	0.21	0.08	0.04	0.03	0.02	0.02
2019-12	95.11	3.25	0.85	0.24	0.16	0.19	0.07	0.04	0.03	0.02	0.02
2020-01	94.61	3.74	0.85	0.24	0.15	0.21	0.07	0.06	0.03	0.02	0.02

Reference: http://gs.statcounter.com/os-market-share/mobile/pakistan

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

CYBER INVESTIGATIONS AGAINST MOBILE DEVICES (CONT’D)…

MOBILE ATTACK DEMONSTRATION



Binding malware with a legitimate application hosted over various open market places.

Malicious App Will Intrude:

- ✓ SMS (Dump, Send/Receive)
- ✓ Call Log
- ✓ Gallery
- ✓ Live Camera
- ✓ Microphone, Contact Directory,
- ✓ Location Tracking etc.

Malicious App Contains:

- ✓ Reverse Back Connection
- ✓ Intruder IP
- ✓ Intruder Port

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

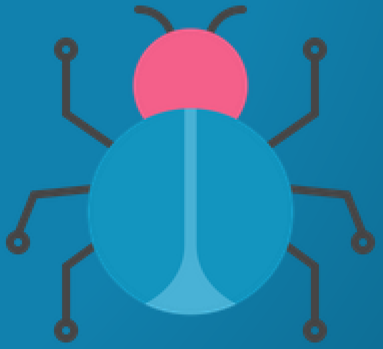
Next Gen Cyber Blunders By Experts

NEXT GEN CYBER BLUNDERS BY EXPERTS

Implementing the security controls is not the only solution for enhancing organization from the security point of view, there are several tuning which may require to be implemented by the experts of those system which may include but not limited to:

If we discuss about security solution, the ideal scenario for all the organization providing critical services would be as follow:

1. An **endpoint solution** is implemented through out the organization;
2. A Security Incident & Event Management solution **(SIEM)** is implemented to monitor critical server(s) and applications;
3. Intelligent **Firewall** for network traffic monitoring;
4. **SPAM filter** for controlling SPAMMING and SPAMMERS;



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NEXT GEN CYBER BLUNDERS BY EXPERTS (CONT'D)…

SIEM SOLUTION: Securing organization by pushing up a notification of suspicious event in order to preventing from data breaches.
I would like to add one thing whether your SIEM solution is capable for monitoring such event or not?

S. No	Event Name	Event Description	Event ID
RANSOMWARE			
1	Object Access	An attempt was made to access a file	4663
2	Sensitive Privilege Use	When user exercise privileges assign to them	4673
3	Process Creation	A process is create when a process is created	4688
4	Process Termination	A process is terminate when a process is terminated	6889
5	Process Special Logon	Special privileges assign to new logon	4672
TROJAN			
6	Trojan Detected	Indicates that Trojan was detected	6008
7	Service Control Manager	The Windows Defender Services entered the stopped state	7036
8	Remote Access	Indicate that backdoor was created	6002
9	Sending E-mail	Hostile Email was attached	6003

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NEXT GEN CYBER BLUNDERS BY EXPERTS (CONT’D)…

SIEM SOLUTION: Securing organization by pushing up a notification of suspicious event in order to preventing from data breaches.
I would like to add one thing whether your SIEM solution is capable for monitoring such event or not?

S. No	Event Name	Event Description	Event ID
		WORMS	
10	Service Installed	An unknown service was installed in the system	4697
11	File Share	A network object was accessed	5140
12	File Share	A network object was added	5142
13	Bootnet DNS interception	Redirect the traffic to malicious site	338301
14	Bootnet Destination blacklist	Access to malicious site	338004

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NEXT GEN CYBER BLUNDERS BY EXPERTS (CONT’D)…

SIEM SOLUTION CRITICAL SUSPICIOUS EVENT ID’S

VIRUS			
15	Malicious software	Indicates a virus	6004
16	Content scan	An attampt was made to scan the content present in system	6010
17	Disk-Bad block	Area of storage that is no longer reliable for storing and retriving data	7
18	Disk-Disk error during paging	Error occurs when your computer swaps information to or from the disk.	51
19	Disk-imminent disk failure	Hard drive failure	52
20	Application Error	An attempt was made to crash the application	1000
SPYWARE			
21	Spyware Detected	Indicates a spyware was detected	6009
22	Service Control Manager	Indicates a new service local synchronization host was installed	7045
23	Service control Manger	Indicates local synchronization host service entered the running state	7036
24	System Logon	Logon session was created to logon to local computer	4624
25	User Account Mangement	An attempt was made to reset the account's password	4724

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NEXT GEN CYBER BLUNDERS BY EXPERTS (CONT’D)…

SIEM SOLUTION CRITICAL SUSPICIOUS EVENT ID’S

ADWARES			
26	Software Install	Indicates that software was installed	11707
27	Software Uninstall	Indicates that software was uninstalled	11724
ADORE ROOTKIT			
28	object Access Request	When an application attempt to access the obejct	4656
29	Changed Object Permission	Someone made changes to access control list of object	4670
30	Object Access	An attempt was made to access any object like kernel	4663
HACKER DEFENDER ROOTKIT			
31	Process Create	A new process has been created	4688
32	Registry	Registry valued was modified	4657
33	Application Error	An attempt was made to crash the application	1000

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

NEXT GEN CYBER BLUNDERS BY EXPERTS (CONT'D)…

SIEM SOLUTION CRITICAL SUSPICIOUS EVENT ID'S

STONED BOOTKIT			
34	Service Control manager	The Protected Storage service failed to start due to the following error: The system cannot find the path specified.	7000
35	Active Directory Doamin Service	An internal asynchronous attempt to update the schema cache failed with an error.	1208
36	System -Drives	The Boot-Start or System-Drives are failed to load	7026
DNS CHANGER EXPLOIT KIT			
37	Remote Access	Remote Desktop Services accepted a connection from IP address	1158
38	DNS	an attempt was made to update them with the new records through dynamic update	6702
39	Application	C:\Program Files\Microsoft Silverlight\slup.exe cannot be restarted	10010

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Compromise Assessment Checklist

COMPROMISE ASSESSMENT CHECKLIST

An advance level compromise assessment activity includes but not limited to the following which helps an organization to identify the scale of compromise.

S. No	Control Name	Objective	Technique	Status	
				Yes	No
		Compromise Assessment Checklist			
1	User Access Control	Assessing the User Access Privilege rights for the OS.	Review of Access right form		
2	Searching for Cracked OS	Assessment of OS by examining its serial no.	Product key viewer/ key finder		
	Searching for Outdated, Obsoleted, End of Life OS	Assessing OS version and Firmware, release issued officially by the vendor	Winver (Windows) uname -a (Linux)		
3	Anti Virus/End point/Defender real time protection	Ensure that the AV/End points real time protection is turned on	Manual technique		
4	AV/Endpoint/OS Updates	Ensure that the AV/End points are Up to dated.	Manual technique		
5	Cracked tools	Assessment of any cracked tool installation (MS Office, Acrobat, IDM, etc.)	Examining installed programs		
6	Open Source tools	Assessment of any open source tool installation (Firefox, VLC, VEEAM, Chrome etc.)	Manual technique		
7	Browser Plug-ins	Assessment of Installed plug-ins in the browser (Video Downloader, File Converter etc.)	Manual technique		
8	Application Activity Monitoring	Assessment of activity performs by examining processes of the application(s)	Process Monitor Apps (procmon, ps -a) Wireshark		

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)...

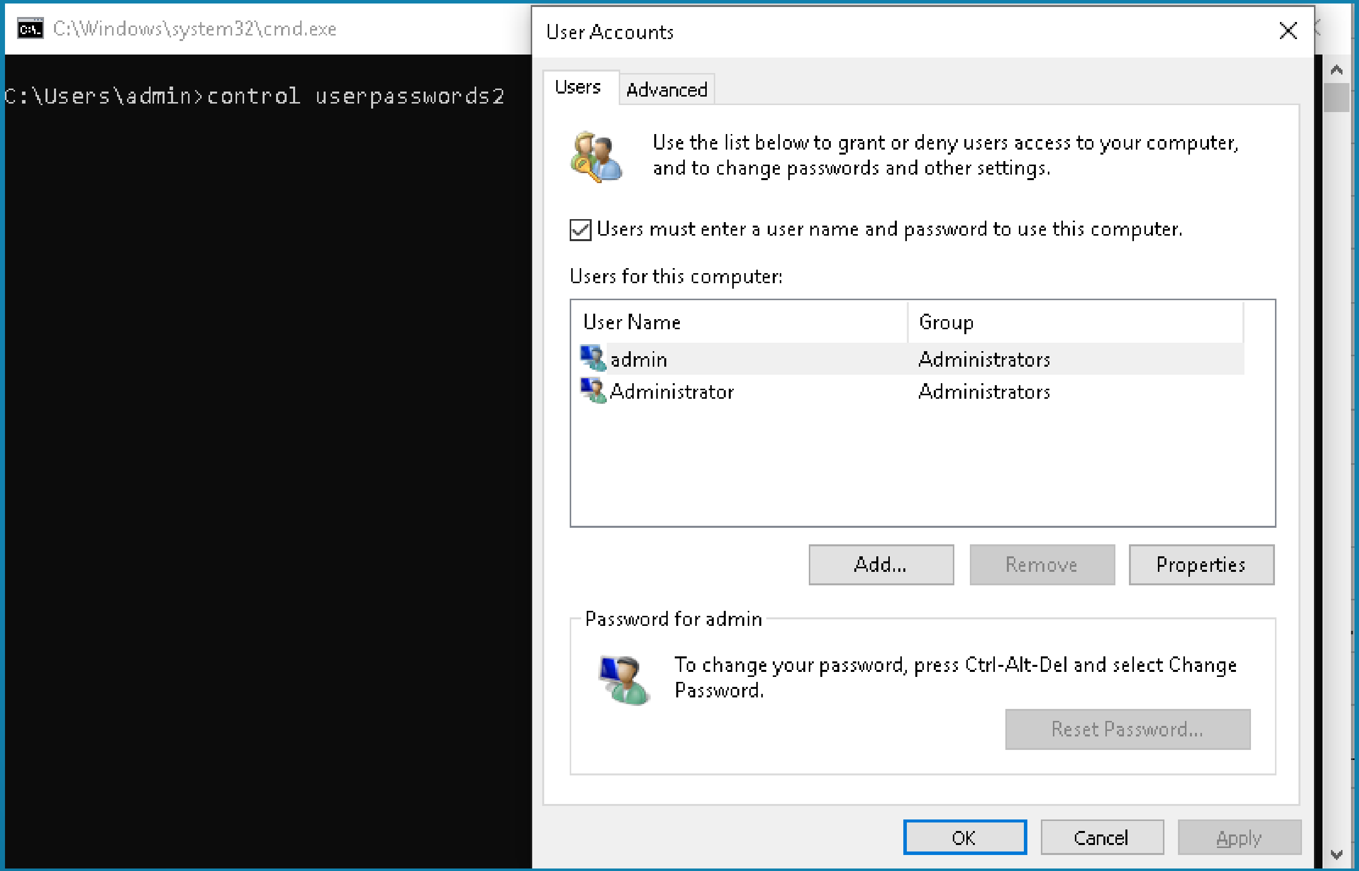
An advance level compromise assessment activity includes but not limited to the following which helps an organization to identify the scale of compromise.

S. No	Control Name	Objective	Technique	Status	
				Yes	No
		Compromise Assessment Checklist			
9	Email/USB Attachments	Assessment of malwares, Trojans, Macros attached in email/USB attachments transferred in the system.			
10	Key logger	Assessment of Malwares, key logger/Spying tools and Trojans .	Manual technique		
11	Java Auto Run	Reviewing installation of java in the system in order to assess auto execution capability of java applets, scripts, java runtime environment files	Manual technique		
12	Shells	Searching for connections (Listening, Established)	netstat -a, netstat -bano (Windows) ss -tulw, ss-tulwn (linux)		
13	Unnecessary Port Assessment	Searching for unnecessary ports opened on the server	netstat, NMAP		
14	Searching for Stored Credentials	Searching for Stored Credential in Windows, Browsers, Applications	rundll32.exe keymgr.dll,KRshowKeyMgr		
15	Network Monitoring	Assess Network Behavior	Nmon		

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)...

USER ACCESS CONTROL - Assessing the User Access Privilege rights for the OS.



C:\Windows\system32\cmd.exe

```
C:\Users\admin>control userpasswords2
```

User Accounts

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☑ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
admin	Administrators
Administrator	Administrators

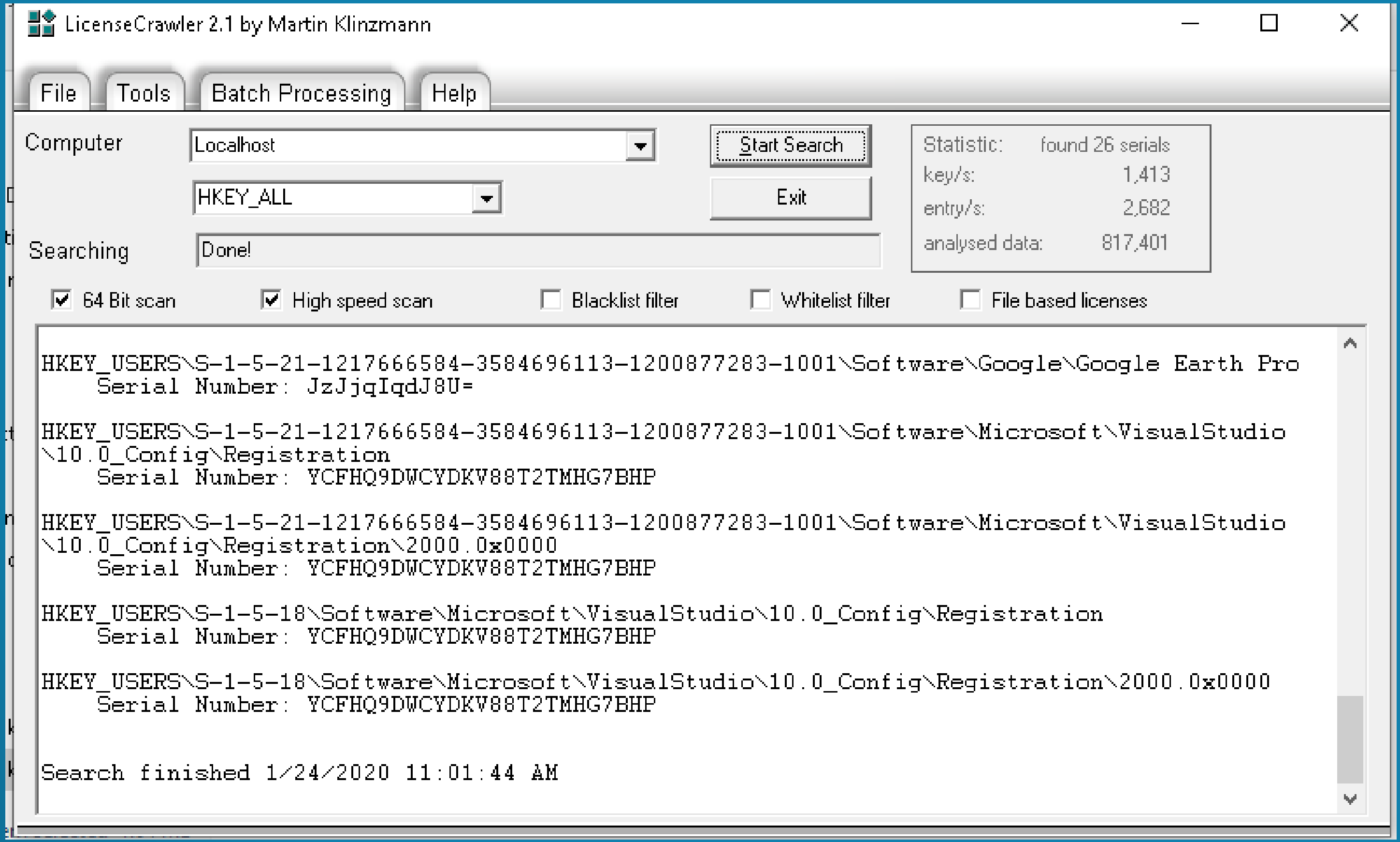
Password for admin

To change your password, press Ctrl-Alt-Del and select Change Password.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)…

SEARCHING FOR CRACKED OS - Assessment of OS by examining its serial no.



Computer: Localhost

HKEY_ALL

Searching: Done!

Statistic: found 26 serials
key/s: 1,413
entry/s: 2,682
analysed data: 817,401

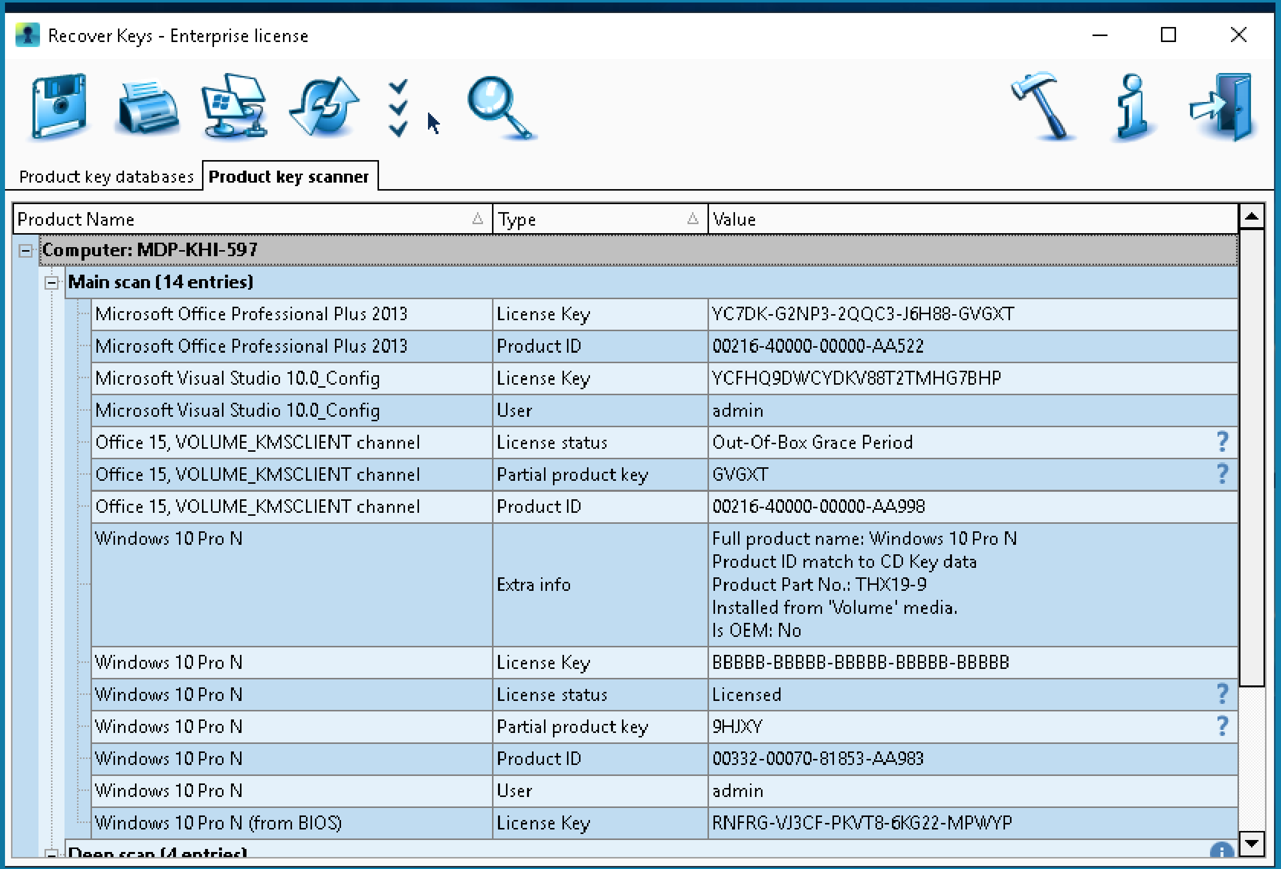
☑ 64 Bit scan ☑ High speed scan □ Blacklist filter □ Whitelist filter □ File based licenses

```
HKEY_USERS\S-1-5-21-1217666584-3584696113-1200877283-1001\Software\Google\Google Earth Pro
    Serial Number: JzJjqIqdJ8U=

HKEY_USERS\S-1-5-21-1217666584-3584696113-1200877283-1001\Software\Microsoft\VisualStudio
\10.0_Config\Registration
    Serial Number: YCFHQ9DWCYDKV88T2TMHG7BHP

HKEY_USERS\S-1-5-21-1217666584-3584696113-1200877283-1001\Software\Microsoft\VisualStudio
\10.0_Config\Registration\2000.0x0000
    Serial Number: YCFHQ9DWCYDKV88T2TMHG7BHP

HKEY_USERS\S-1-5-18\Software\Microsoft\VisualStudio\10.0_Config\Registration
    Serial Number: YCFHQ9DWCYDKV88T2TMHG7BHP

HKEY_USERS\S-1-5-18\Software\Microsoft\VisualStudio\10.0_Config\Registration\2000.0x0000
    Serial Number: YCFHQ9DWCYDKV88T2TMHG7BHP


Search finished 1/24/2020 11:01:44 AM
```

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)…

SEARCHING FOR CRACKED APPLICATION(S) - Assessment of any cracked tool installation (MS Office, Acrobat, IDM, etc.)



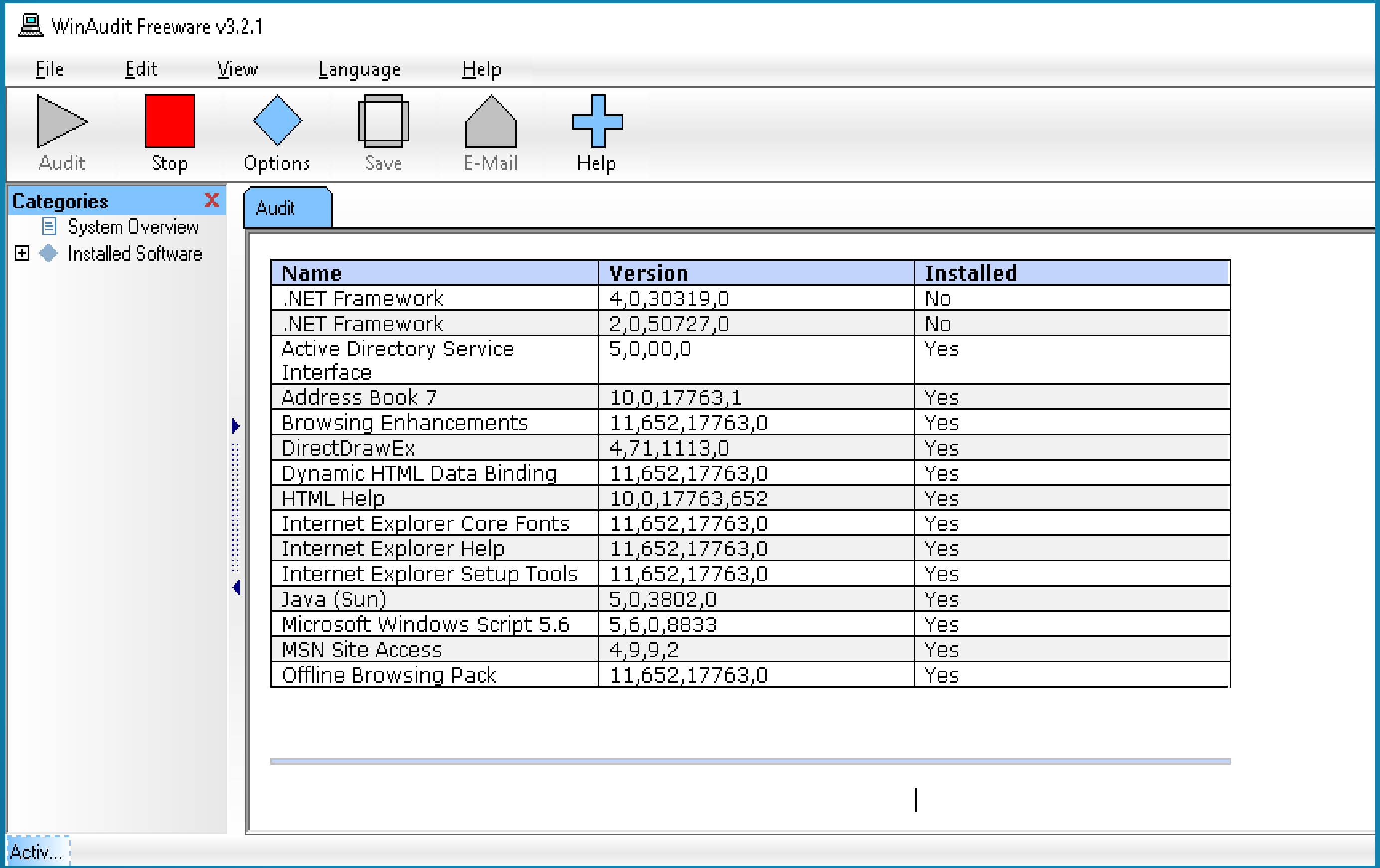
Recover Keys - Enterprise license

Product Name	Type	Value
Computer: MDP-KHI-597		
Main scan (14 entries)		
Microsoft Office Professional Plus 2013	License Key	YC7DK-G2NP3-2QQC3-J6H88-GVGXT
Microsoft Office Professional Plus 2013	Product ID	00216-40000-00000-AA522
Microsoft Visual Studio 10.0_Config	License Key	YCFHQ9DWCYDKV88T2TMHG7BHP
Microsoft Visual Studio 10.0_Config	User	admin
Office 15, VOLUME_KMSCLIENT channel	License status	Out-Of-Box Grace Period ?
Office 15, VOLUME_KMSCLIENT channel	Partial product key	GVGXT ?
Office 15, VOLUME_KMSCLIENT channel	Product ID	00216-40000-00000-AA998
Windows 10 Pro N	Extra info	Full product name: Windows 10 Pro N Product ID match to CD Key data Product Part No.: THX19-9 Installed from 'Volume' media. Is OEM: No
Windows 10 Pro N	License Key	BBBBB-BBBBB-BBBBB-BBBBB-BBBBB
Windows 10 Pro N	License status	Licensed ?
Windows 10 Pro N	Partial product key	9HJXY ?
Windows 10 Pro N	Product ID	00332-00070-81853-AA983
Windows 10 Pro N	User	admin
Windows 10 Pro N (from BIOS)	License Key	RNFRG-VJ3CF-PKVT8-6KG22-MPWYP
Deep scan (4 entries)		

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)…

SEARCHING FOR OBSELETED/OUTDATED APPLICATION(S)/OS - Assessing OS version and Firmware, release issued officially by the vendor.

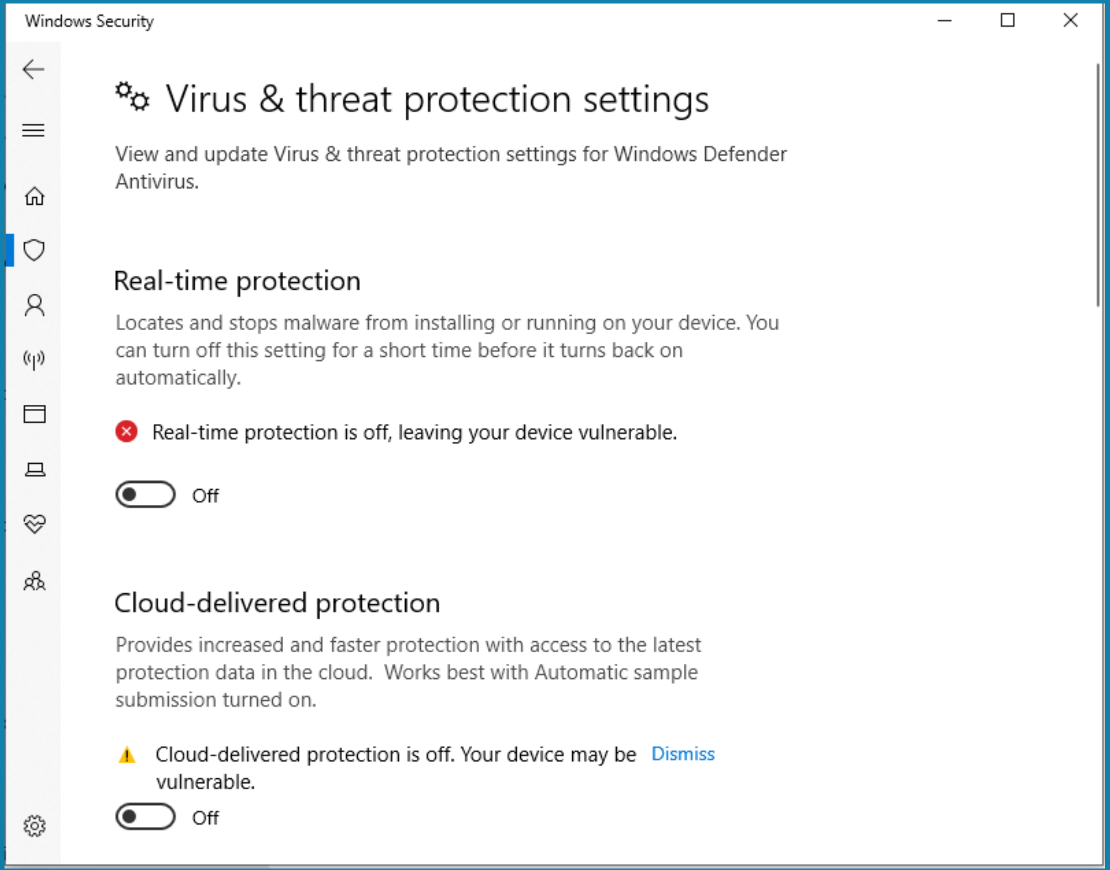


Name	Version	Installed
.NET Framework	4,0,30319,0	No
.NET Framework	2,0,50727,0	No
Active Directory Service Interface	5,0,00,0	Yes
Address Book 7	10,0,17763,1	Yes
Browsing Enhancements	11,652,17763,0	Yes
DirectDrawEx	4,71,1113,0	Yes
Dynamic HTML Data Binding	11,652,17763,0	Yes
HTML Help	10,0,17763,652	Yes
Internet Explorer Core Fonts	11,652,17763,0	Yes
Internet Explorer Help	11,652,17763,0	Yes
Internet Explorer Setup Tools	11,652,17763,0	Yes
Java (Sun)	5,0,3802,0	Yes
Microsoft Windows Script 5.6	5,6,0,8833	Yes
MSN Site Access	4,9,9,2	Yes
Offline Browsing Pack	11,652,17763,0	Yes

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)...

ENSURING ENDPOINT/ANTIVIRUS/DEFENDER PROTECTION - Ensure that the AV/End points real time protection is turned on.



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

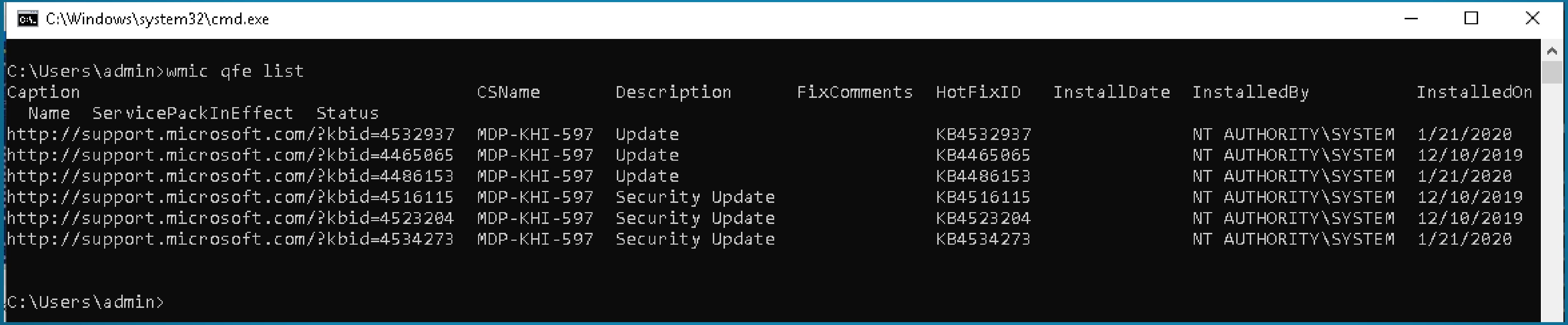
Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Off

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)...

ENSURING AV/ENDPOINT/OS UPDATES - Ensure that the OS/AV/End points are up to dated.

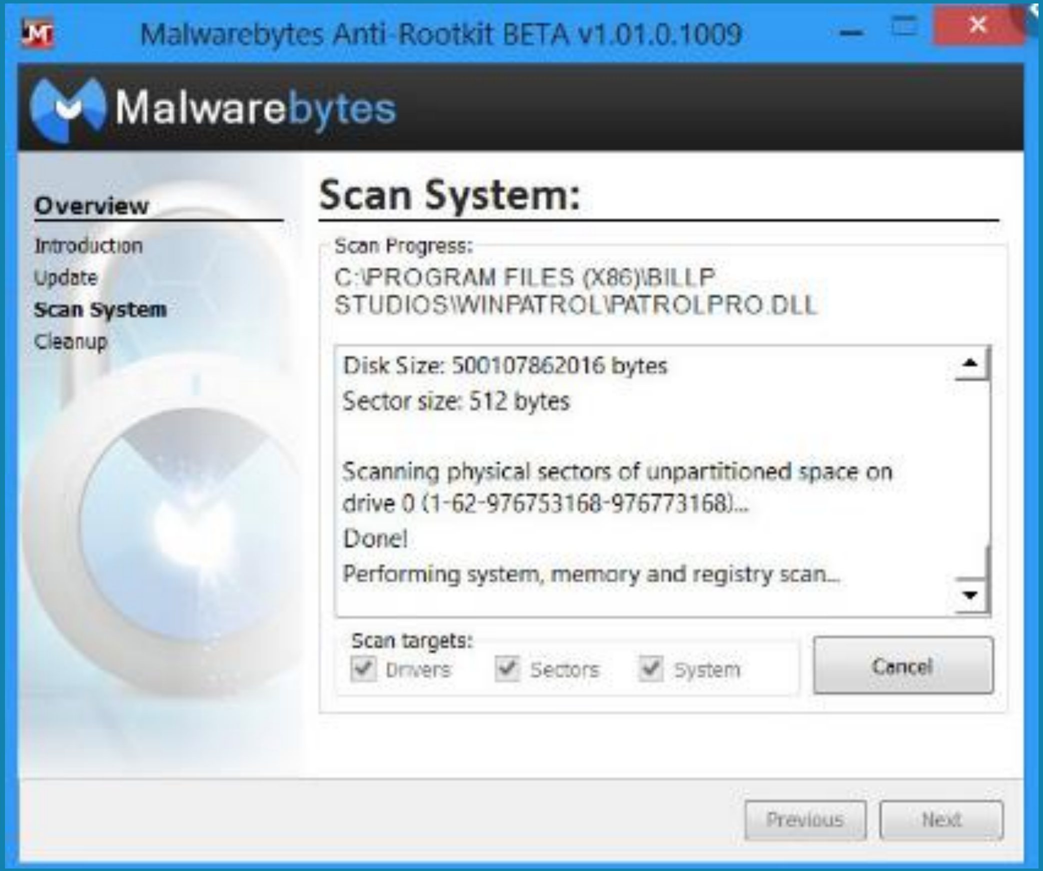


```
C:\Users\admin>wmic qfe list
Caption                                     CSName         Description      FixComments  HotFixID   InstallDate  InstalledBy          InstalledOn
  Name  ServicePackInEffect  Status
http://support.microsoft.com/?kbid=4532937  MDP-KHI-597  Update                          KB4532937               NT AUTHORITY\SYSTEM  1/21/2020
http://support.microsoft.com/?kbid=4465065  MDP-KHI-597  Update                          KB4465065               NT AUTHORITY\SYSTEM  12/10/2019
http://support.microsoft.com/?kbid=4486153  MDP-KHI-597  Update                          KB4486153               NT AUTHORITY\SYSTEM  1/21/2020
http://support.microsoft.com/?kbid=4516115  MDP-KHI-597  Security Update                 KB4516115               NT AUTHORITY\SYSTEM  12/10/2019
http://support.microsoft.com/?kbid=4523204  MDP-KHI-597  Security Update                 KB4523204               NT AUTHORITY\SYSTEM  12/10/2019
http://support.microsoft.com/?kbid=4534273  MDP-KHI-597  Security Update                 KB4534273               NT AUTHORITY\SYSTEM  1/21/2020


C:\Users\admin>
```

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)…

DETECTING KEYLOGGERS & MALICIOUS FILES - Assessment of Malwares, key logger/Spying tools and Trojans .



Scan System:

Scan Progress:
C:\PROGRAM FILES (X86)\BILLP STUDIOS\WINPATROL\PATROLPRO.DLL

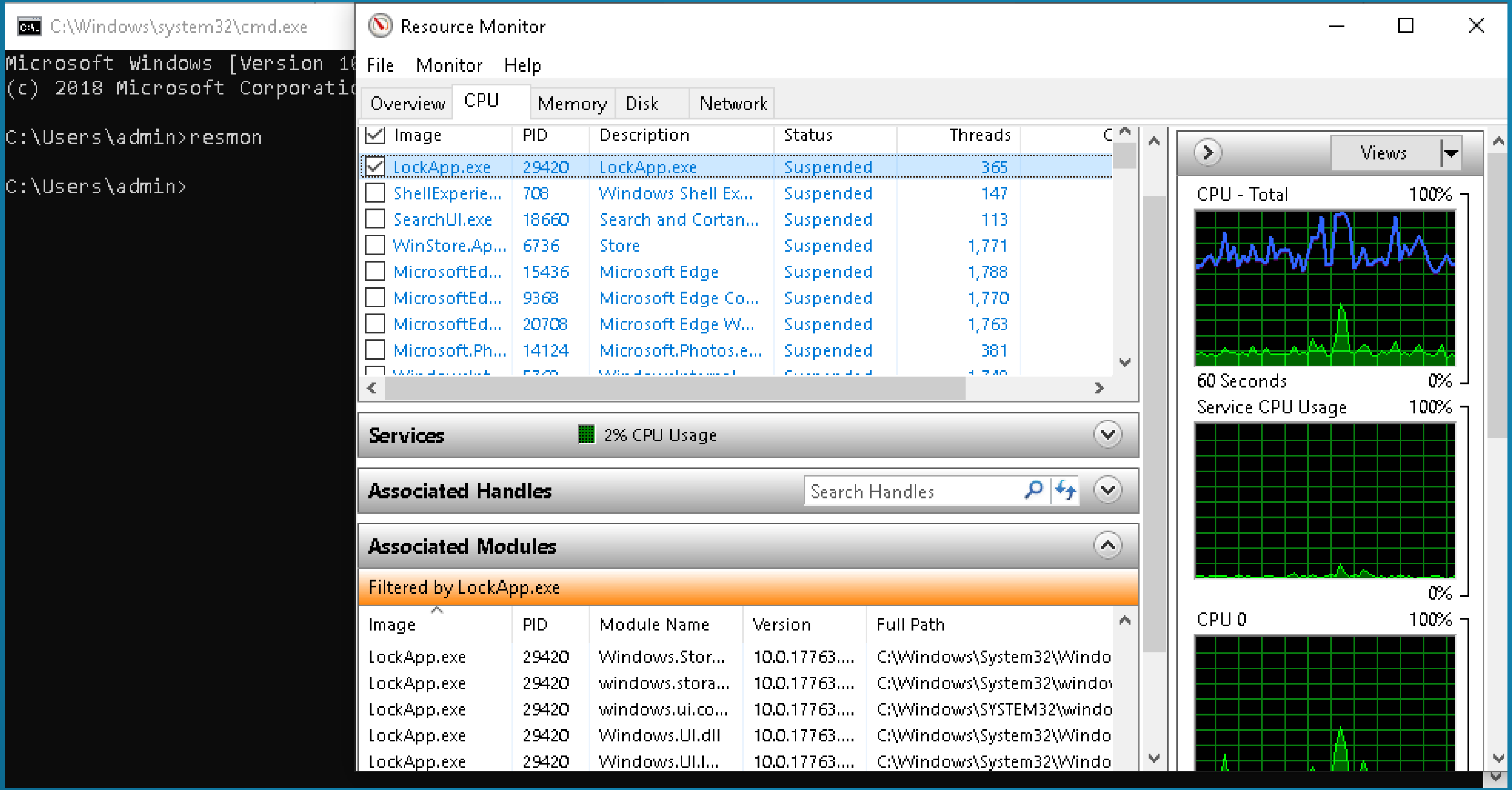
```
Disk Size: 500107862016 bytes
Sector size: 512 bytes

Scanning physical sectors of unpartitioned space on
drive 0 (1-62-976753168-976773168)...
Done!
Performing system, memory and registry scan...
```

Scan targets: ☑ Drivers ☑ Sectors ☑ System

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)...

DETECTING KEYLOGGERS & MALICIOUS FILES - Assessment of Malwares, key logger/Spying tools and Trojans .



```
Microsoft Windows [Version 1(
(c) 2018 Microsoft Corporatio

C:\Users\admin>resmon

C:\Users\admin>
```

☑ Image	PID	Description	Status	Threads
☑ LockApp.exe	29420	LockApp.exe	Suspended	365
□ ShellExperie...	708	Windows Shell Ex...	Suspended	147
□ SearchUI.exe	18660	Search and Cortan...	Suspended	113
□ WinStore.Ap...	6736	Store	Suspended	1,771
□ MicrosoftEd...	15436	Microsoft Edge	Suspended	1,788
□ MicrosoftEd...	9368	Microsoft Edge Co...	Suspended	1,770
□ MicrosoftEd...	20708	Microsoft Edge W...	Suspended	1,763
□ Microsoft.Ph...	14124	Microsoft.Photos.e...	Suspended	381

Services 🟩 2% CPU Usage

Associated Handles

Associated Modules

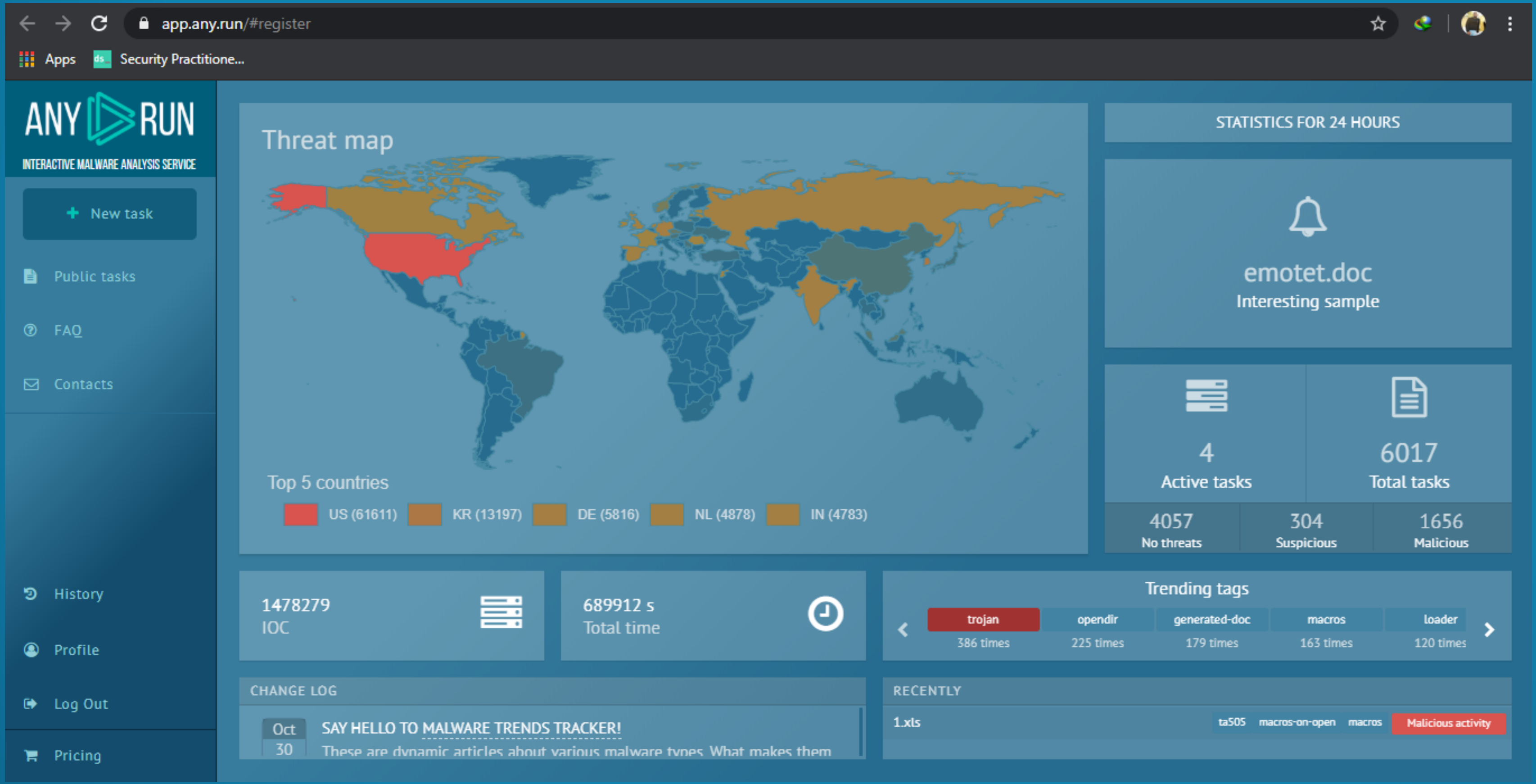
Filtered by LockApp.exe

Image	PID	Module Name	Version	Full Path
LockApp.exe	29420	Windows.Stor...	10.0.17763....	C:\Windows\System32\Windo
LockApp.exe	29420	windows.stora...	10.0.17763....	C:\Windows\System32\windo
LockApp.exe	29420	windows.ui.co...	10.0.17763....	C:\Windows\SYSTEM32\windo
LockApp.exe	29420	Windows.UI.dll	10.0.17763....	C:\Windows\System32\Windo
LockApp.exe	29420	Windows.UI.I...	10.0.17763....	C:\Windows\System32\Windo

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)…

DETECTING KEYLOGGERS & MALICIOUS FILES - Assessment of Malwares, key logger/Spying tools and Trojans .



app.any.run/#register

Apps Security Practitione...

ANY RUN
INTERACTIVE MALWARE ANALYSIS SERVICE

+ New task

Public tasks

FAQ

Contacts

History

Profile

Log Out

Pricing

Threat map

Top 5 countries

🟥 US (61611) 🟫 KR (13197) 🟫 DE (5816) 🟫 NL (4878) 🟫 IN (4783)

STATISTICS FOR 24 HOURS

emotet.doc
Interesting sample

4 Active tasks

6017 Total tasks

4057 No threats

304 Suspicious

1656 Malicious

1478279 IOC

689912 s Total time

Trending tags

trojan	opendir	generated-doc	macros	loader
386 times	225 times	179 times	163 times	120 times

CHANGE LOG

Oct 30 SAY HELLO TO MALWARE TRENDS TRACKER!
These are dynamic articles about various malware types. What makes them

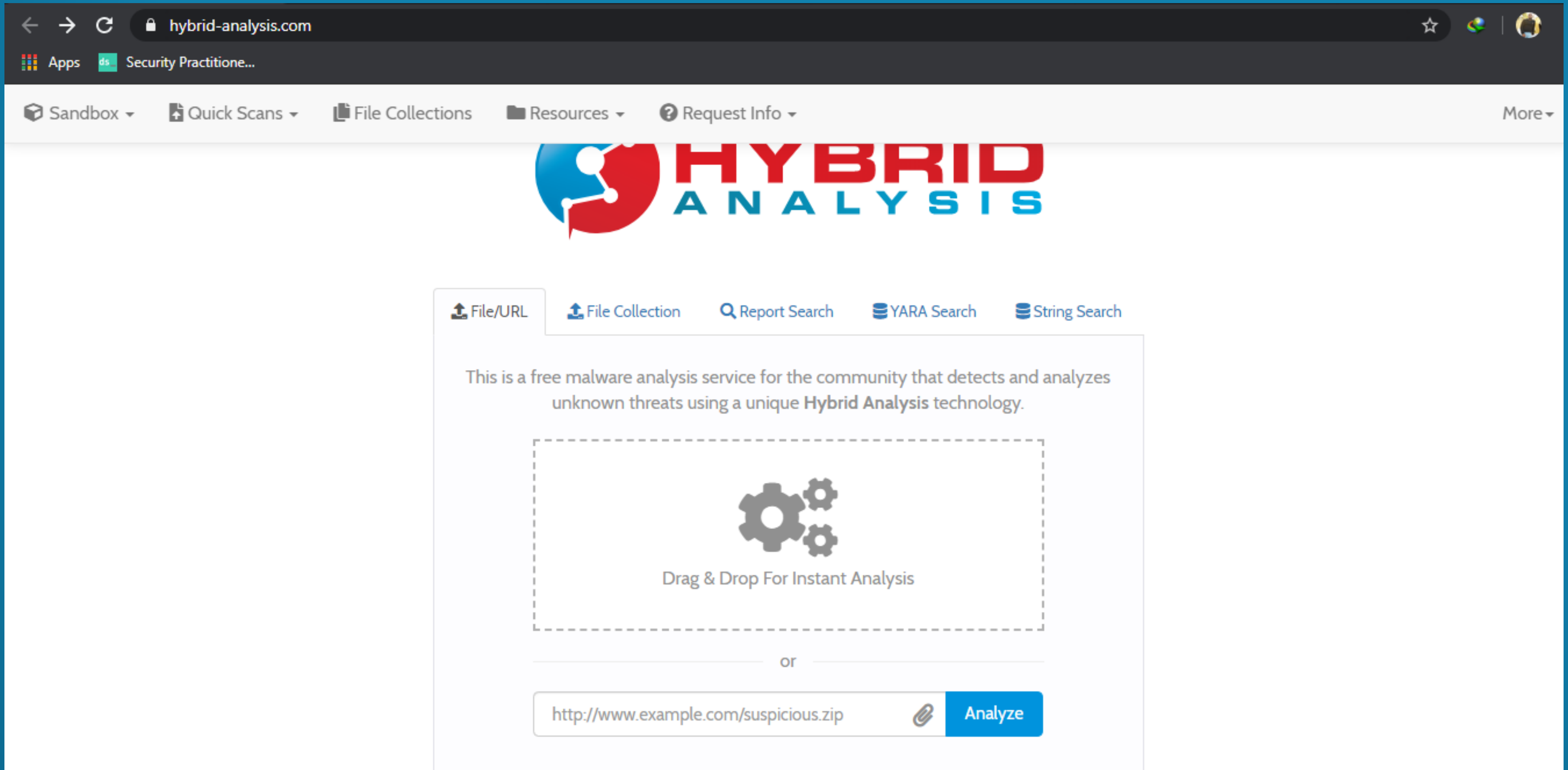
RECENTLY

1.xls ta505 macros-on-open macros Malicious activity

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT’D)...

Email/USB Attachment - Assessment of malwares, Trojans, Macros attached in email/USB attachments transferred in the system.

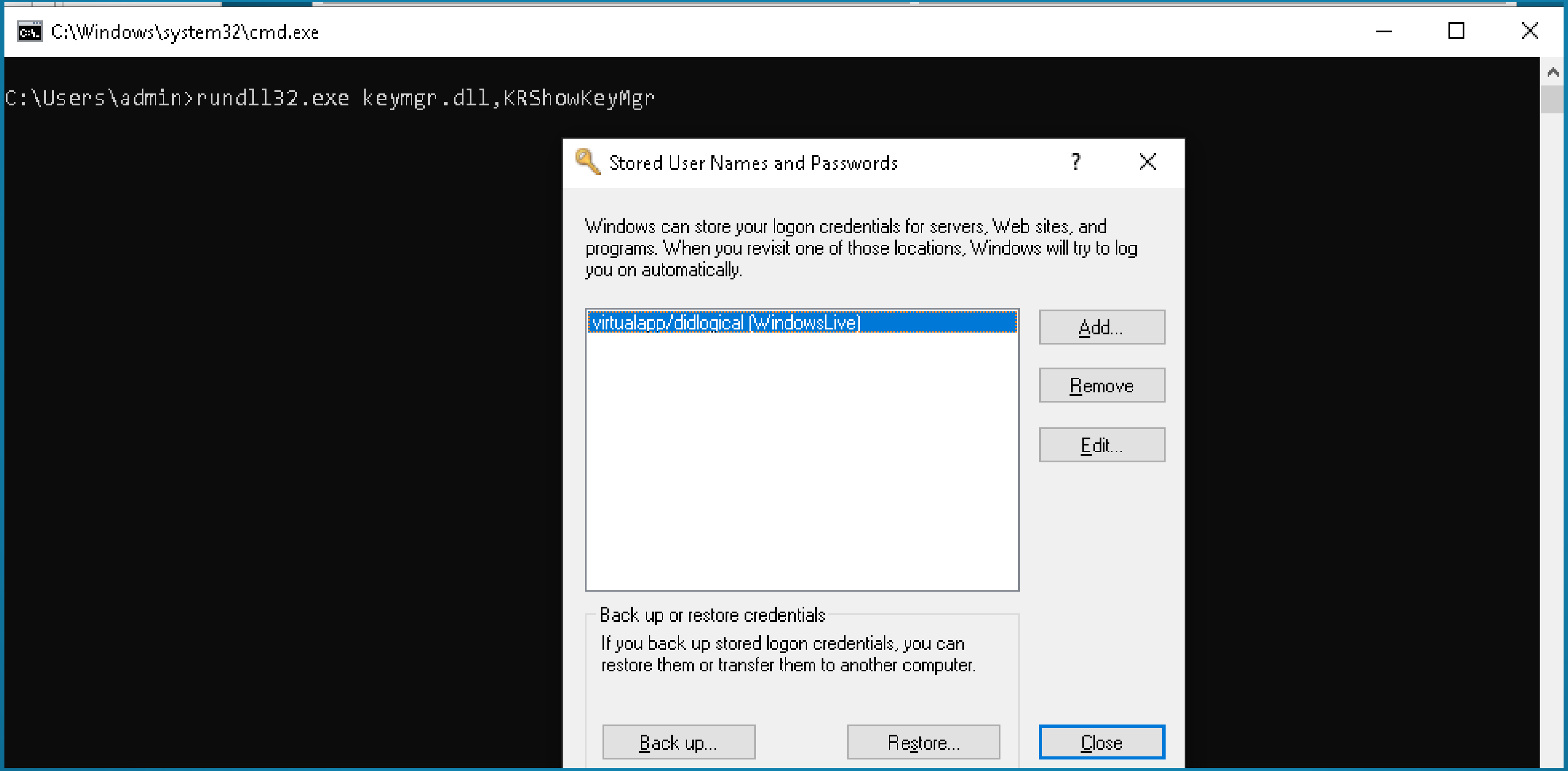


This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)…

Searching for Stored Credentials - Searching for Stored Credential in Windows, Browsers, Applications.



```
C:\Users\admin>rundll32.exe keymgr.dll,KRShowKeyMgr
```

Windows can store your logon credentials for servers, Web sites, and programs. When you revisit one of those locations, Windows will try to log you on automatically.

virtualapp/didlogical (WindowsLive)

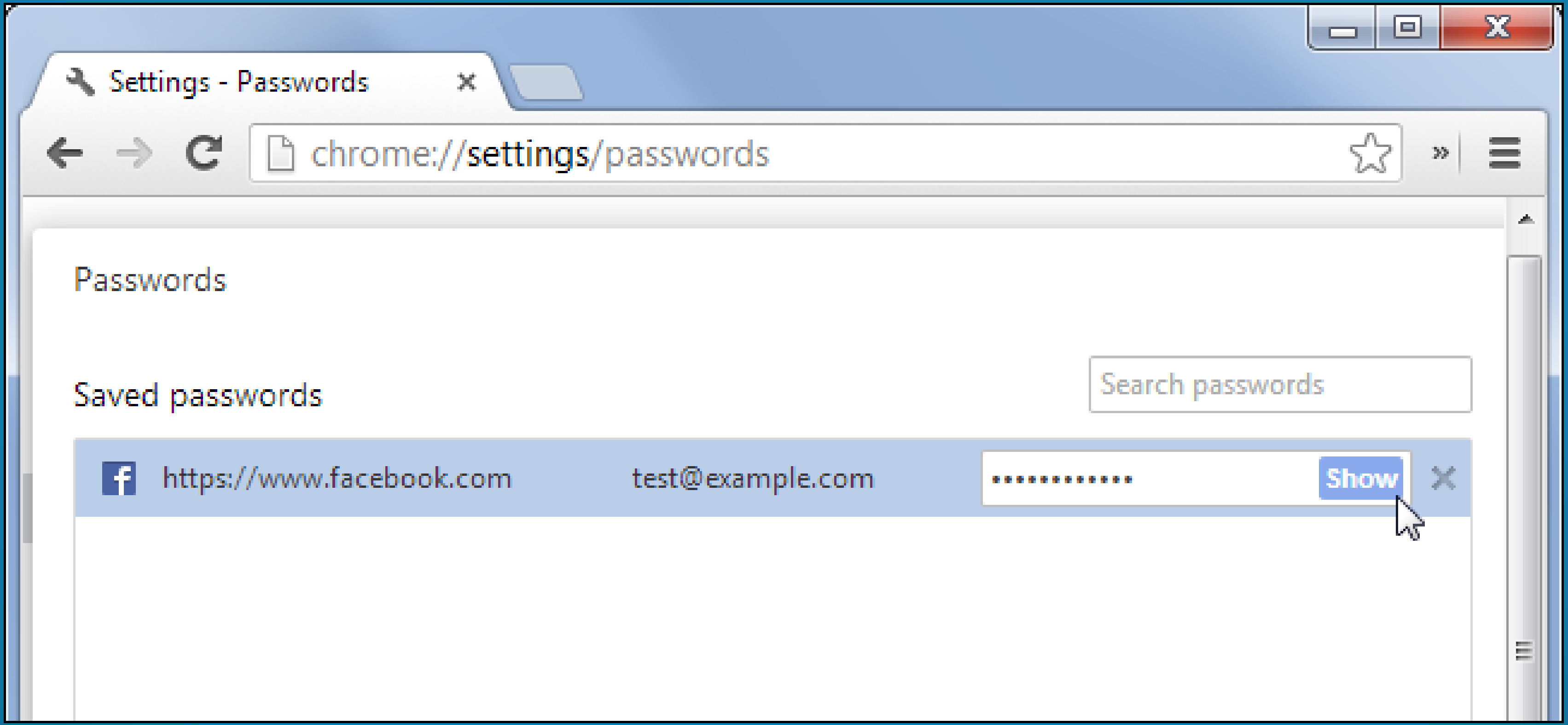
Back up or restore credentials

If you back up stored logon credentials, you can restore them or transfer them to another computer.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

COMPROMISE ASSESSMENT CHECKLIST (CONT'D)…

Searching for Stored Credentials - Searching for Stored Credential in Windows, Browsers, Applications.



Settings - Passwords

chrome://settings/passwords

Passwords

Saved passwords

https://www.facebook.com	test@example.com	•••••••••••••

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

Role Of An Individual During CA

ROLE OF AN INDIVIDUAL DURING CA

Compromise assessment can be performed to detect unknown risks that could have significant consequences (and cost impact) in case of undetected security breaches.
Taking an example of a organization, when an employee newly joined the organization, following are the list of facilities which may provide to the employee as per company policy.

- Desktop/Laptop;
- Email Address;
- Cell Phone / Landline;
- USB Drive;
- Dual Screen Monitor;
- Printers & Scanner.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ROLE OF AN INDIVIDUAL DURING CA

Desktop/Laptop

- Use of Unauthorized software's in company provided system;
- Keeping personal data in the official system;
- Sharing laptop/Desktop password with other team colleagues;
- Running portable applications in the laptop/desktop;
- Sharing/Uploading company’s confidential data;
- Sharing laptops/Desktops with other team members.

Remedial Action(s):

- Avoid using unauthorized software’s and use of authorized software’s as per company policy;
- Avoid keeping personal data in the official system, it may recover;
- Never share your password with other team colleagues;
- Always Lock the system whenever leaving the seat;
- Never share or upload company’s confidential data on any forum or any media;
- Never share your official laptop with other team member for any reason.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ROLE OF AN INDIVIDUAL DURING CA (CONT'D)...

Email Address

- Opening and accessing new arrived emails undeliberately;
- Opening email attachment undeliberately;
- Opening email from unknown source and downloading or clicking the content of the email coming from unknown source;
- Registering official email on suspicious websites and forums;
- Responding to SPAM emails.

Remedial Action(s):

- Always check sender email address while reading email;
- Always scan email attachment from Anti Virus software first;
- Never open email or any attachment arrived from unknown source it can affect the system and may also breach data;
- Never register official email address on suspicious websites and forums;
- Never respond to SPAM email.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ROLE OF AN INDIVIDUAL DURING CA (CONT'D)…

Cell Phone

- Installing application(s) from uncommon market place;
- Unprotected cell phone (Screen Lock, Pattern);
- Using Cell phone over public WIFI network;
- Operating system/Software's are not updated;
- Responding to SPAM emails;

Landline

- Unprotected dialing facility on landline phone;
- Unrestricted call forwarding facility;

Remedial Action(s):

- Always install application(s) from known market place i.e. (Play Store, Appstore);
- Always protect cell phone by implementing PIN, Pattern lock as the first line of defense;
- Avoid using cell phone over public WIFI network;
- Keep Operating system and Application software's up to dated;
- Never respond to SPAM email via cell phone.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ROLE OF AN INDIVIDUAL DURING CA (CONT’D)…

USB Drive

- Lost of USB Stick can loss of information which can be
- A Financial Information;
- Personal data;
- Confidential company information;
- sharing a USB Stick to a friend;
- The uncontrolled use of removable media can increase the risk of malware being transferred to critical business systems.

Remedial Action(s):

- Limit the use of all removable media devices except when specifically authorized;
- Apply password protection. To safeguard sensitive information and restrict access, all removable media should be protected with strong passwords;
- Never attempt to access files from any removable media that you may have found; It may contain a virus that will infect computer systems with malware.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ROLE OF AN INDIVIDUAL DURING CA (CONT'D)...

Dual Screen Monitor

- Use of Default password of Bluetooth connecting with the monitor;
- Mira Casting option kept on enabled;

Remedial Action(s):

- Don't use default password, Changing the default password is the priority task while network device in the network;
- Mira casting, screen casting, screen mirroring option(s) should be disabled.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ROLE OF AN INDIVIDUAL DURING CA (CONT’D)…

Printer & Scanner

- Use of Default password of Printer Wireless network;
- Carbon copy allowed to be printed from console;

Remedial Action(s):

- Don’t use default password, Changing the default password is the priority task while network device in the network;
- Configure and disable carbon copy printing option from printer console.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

DEMONSTRATION

DEMONSTRATION

The demonstration has been designed to educate the user about ongoing threats that can be used by the intruders to trick the user in order to gain the confidential information from their system.

DEMONSTRATION

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.