Is It Wrong to Try to Find APT Techniques in Ransomware Attack?

Secureworks

Secureworks

Kiyotaka Tamada

Keita Yamazaki

You Nakatsuru

2020/01/17

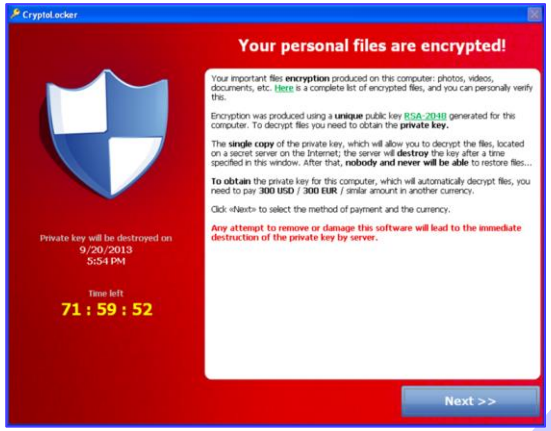
Japan Security Analyst Conference 2020

Agenda

- Overview
- Case Study
- Result of Targeted Ransomware Incident Investigations
    - Tactics, Techniques, and Procedures
        - Initial Access
        - Dominance (Privilege Escalation, Discovery, Lateral Movement)
        - Ransom
        - Anti-Forensics
    - Comparison with Targeted Attack
- Fight Against Targeted Ransomware Incidents
- Summary, and Prediction of Targeted Ransomware

Overview

Trend Changes of Ransomware Incidents



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

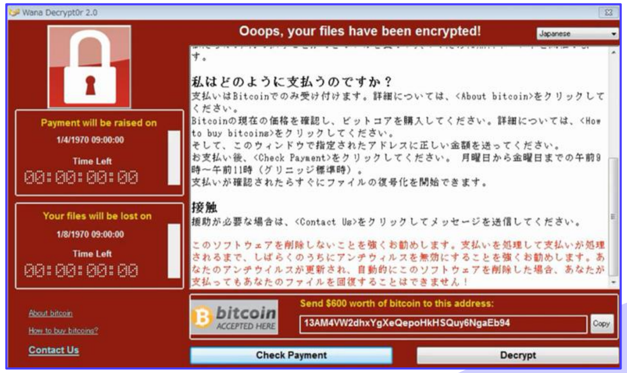
Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/20/2013
5:54 PM

Time left
71 : 59 : 52

CryptoLocker (Sep 2013)



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

す。

私はどのように支払うのですか？

支払いはBitcoinでのみ受け付けます。詳細については、<About bitcoin>をクリックしてください。
Bitcoinの現在の価格を確認し、ビットコアを購入してください。詳細については、<How to buy bitcoins>をクリックしてください。
そして、このウィンドウで指定されたアドレスに正しい金額を送ってください。
お支払い後、<Check Payment>をクリックしてください。 月曜日から金曜日までの午前9時～午前11時（グリニッジ標準時）。
支払いが確認されたらすぐにファイルの復号化を開始できます。

接触

援助が必要な場合は、<Contact Us>をクリックしてメッセージを送信してください。

このソフトウェアを削除しないことを強くお勧めします。支払いを処理して支払いが処理されるまで、しばらくのうちにアンチウィルスを無効にすることを強くお勧めします。あなたのアンチウイルスが更新され、自動的にこのソフトウェアを削除した場合、あなたが支払ってもあなたのファイルを回復することはできません！

Payment will be raised on
1/4/1970 09:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 09:00:00
Time Left
00:00:00:00

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Wannacry (May 2017)

~ 2017

Infected by mail attachment or drive-by download

2017

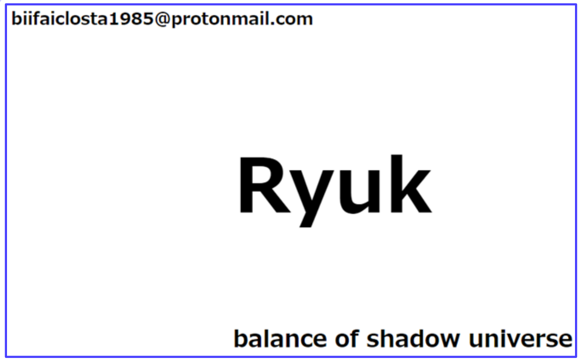
Large scale incident - Wannacry

Organization's infected via public-facing servers vulnerable to MS17-010

2018 ~

More and more cases of attackers manually attacking corporate networks

Change decryption price according to size of organization and whether they have paid in the past

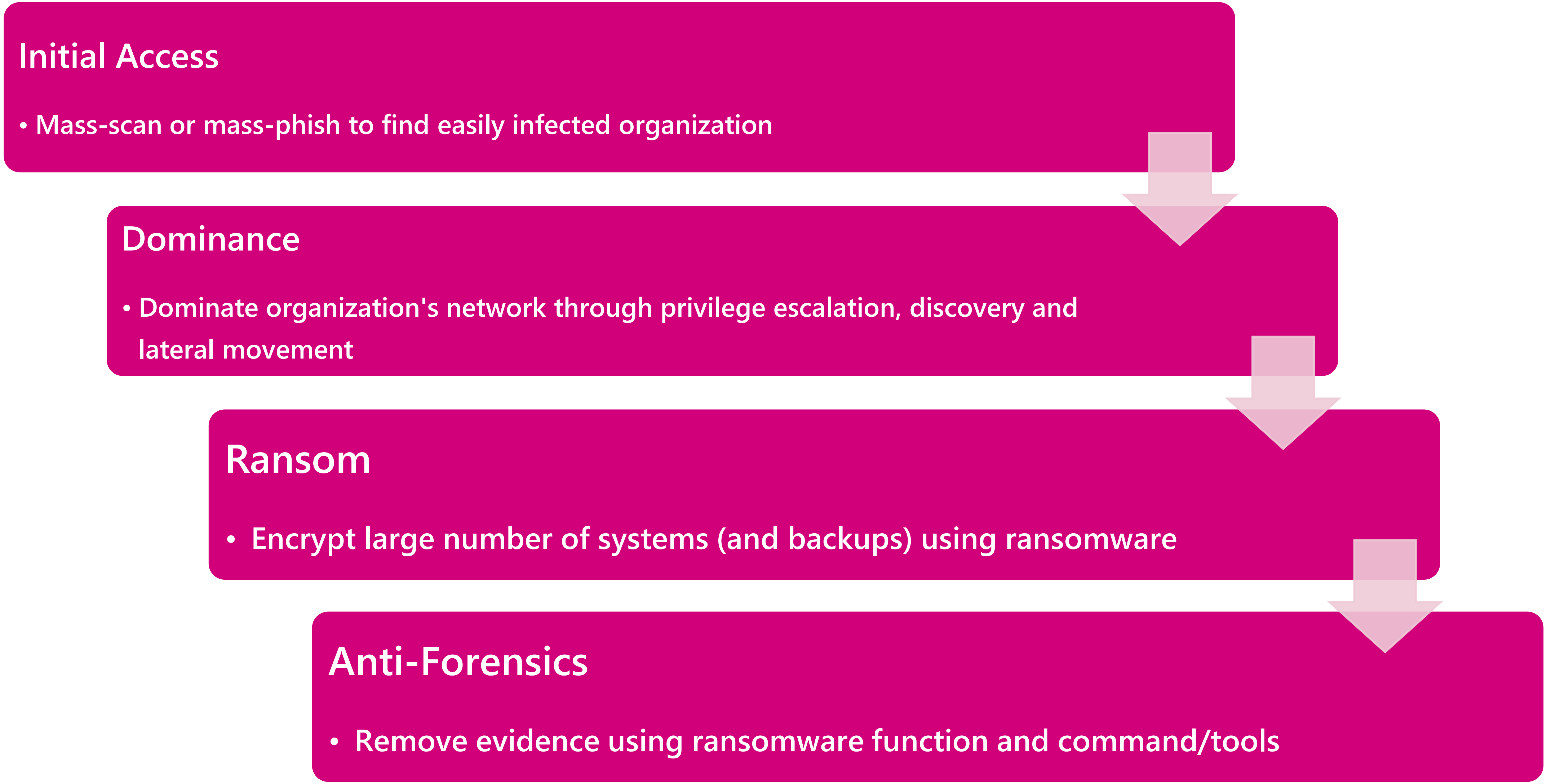


biifaiclosta1985@protonmail.com

Ryuk

balance of shadow universe

Typical Flow of Targeted Ransomware Incident



Initial Access

- Mass-scan or mass-phish to find easily infected organization

Dominance

- Dominate organization's network through privilege escalation, discovery and lateral movement

Ransom

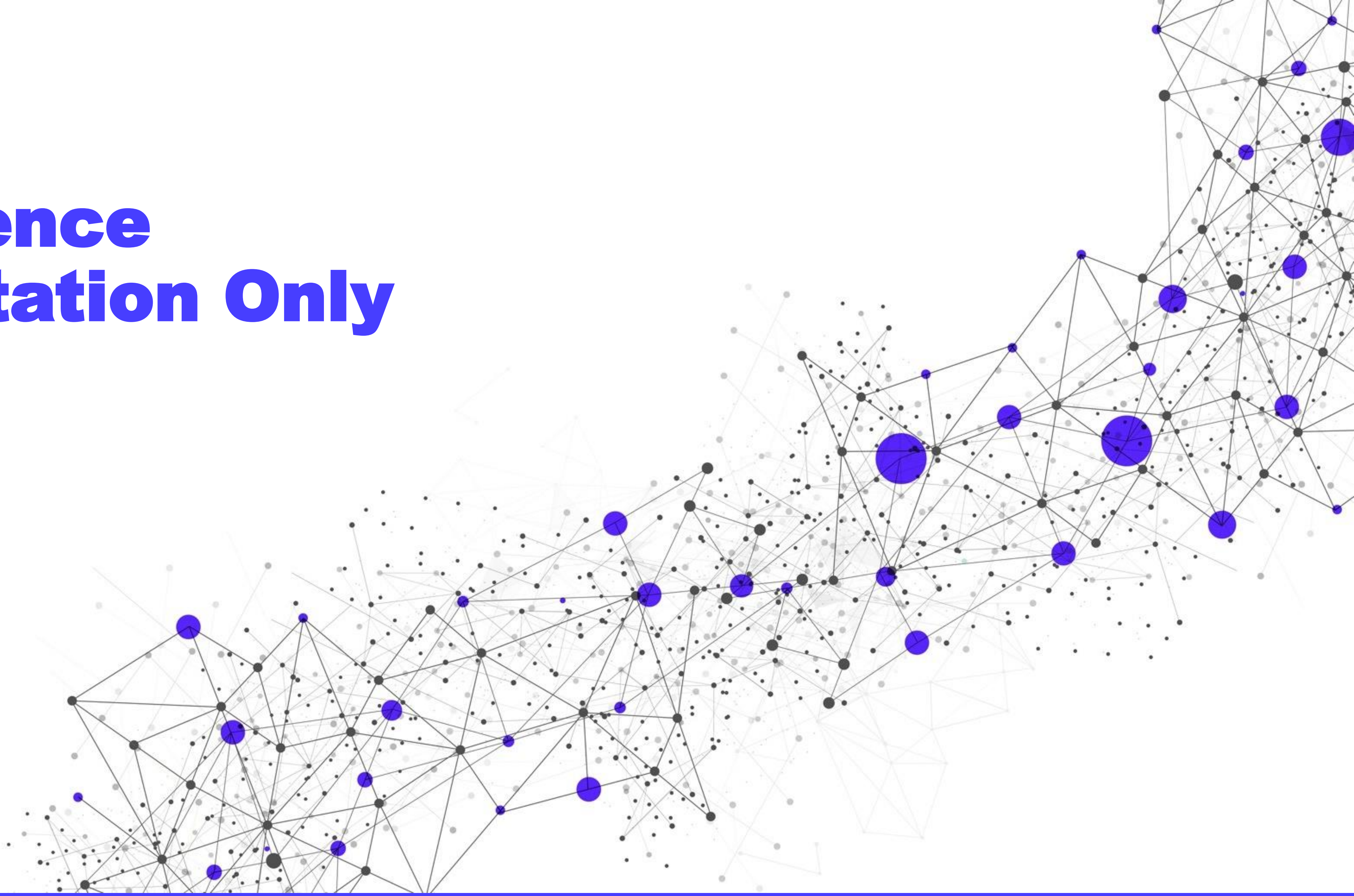
- Encrypt large number of systems (and backups) using ransomware

Anti-Forensics

- Remove evidence using ransomware function and command/tools

Case Study

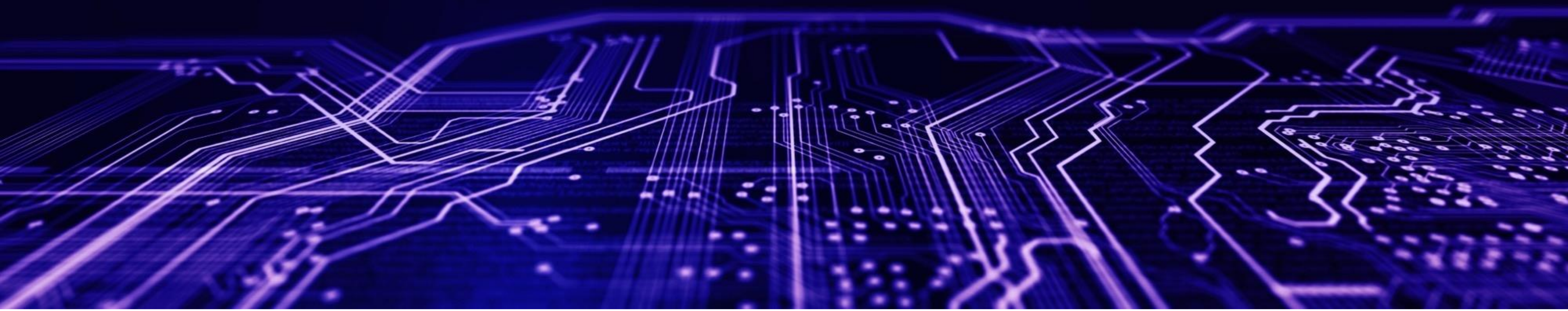
Conference Presentation Only



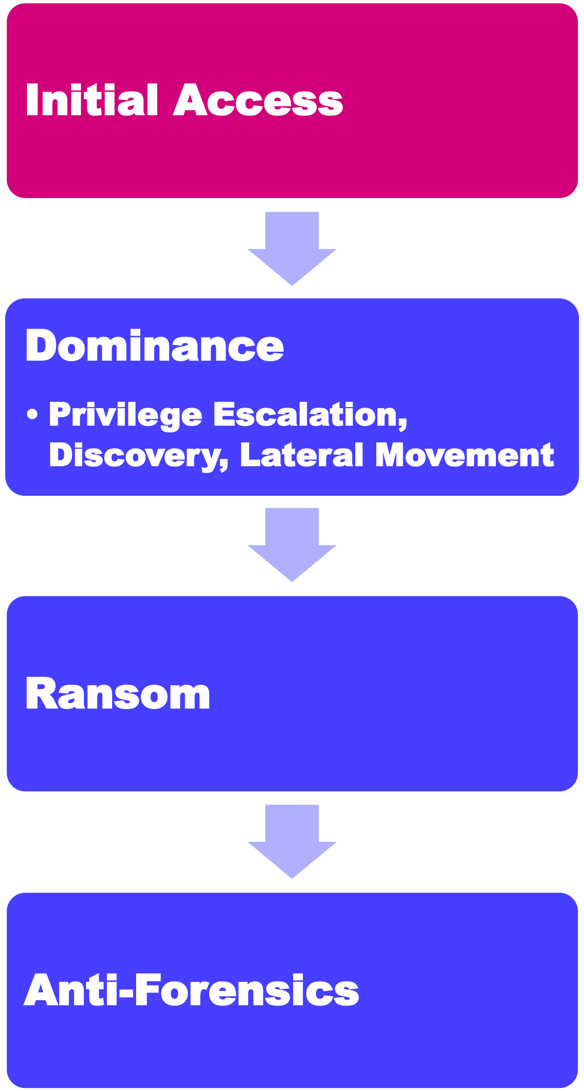
Results of Targeted Ransomware Incident Investigations

Tactics, Techniques, and Procedures

Results of Targeted Ransomware Incident Investigations



Initial Access Techniques



Initial Access

Dominance

- **Privilege Escalation, Discovery, Lateral Movement**

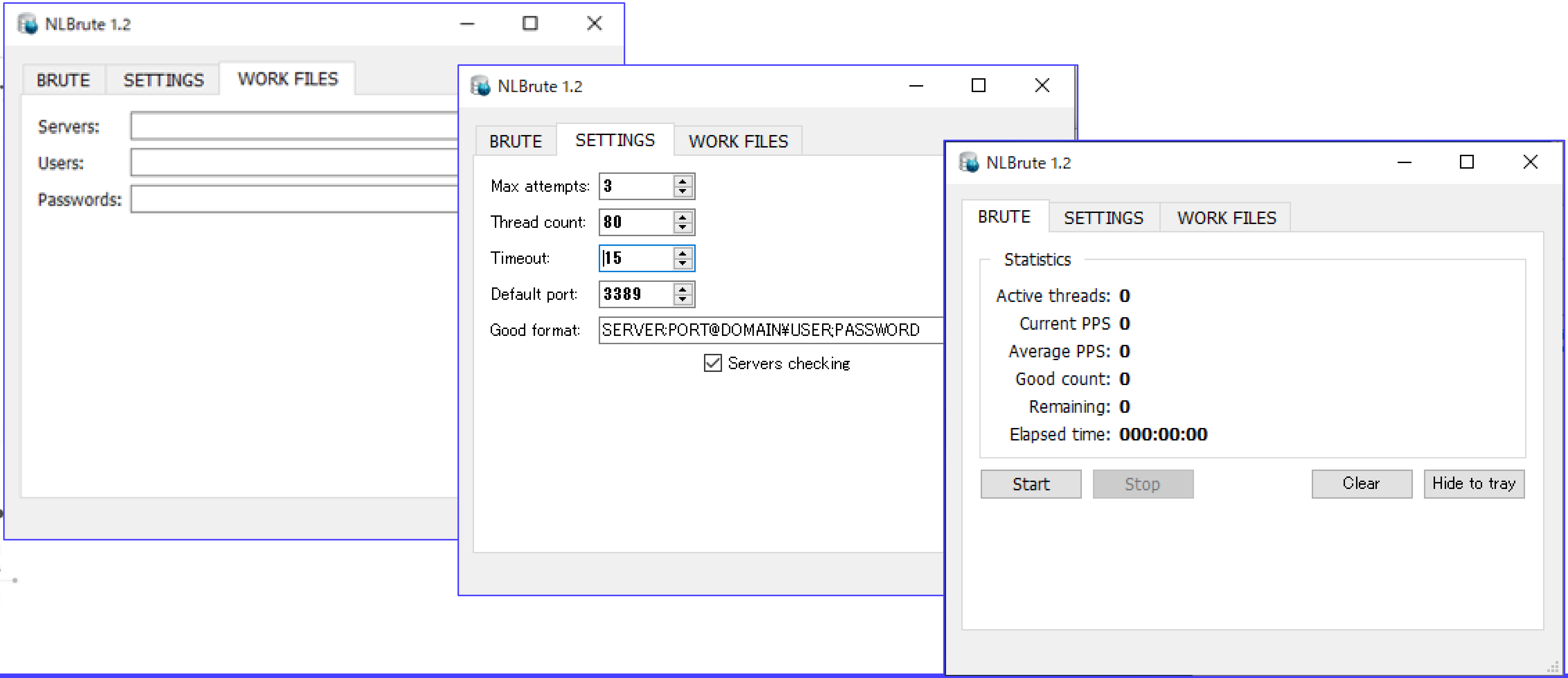
Ransom

Anti-Forensics

- Domestic and overseas cases
  - Via public RDP or VPN
    - Use brute-force tools like NLBrute to identify weak passwords
  - Through malware attached to e-mail
    - Via Emotet (then download TrickBot)
- Only in domestic cases
  - Via portable connection devices assigned global IP address + hosts vulnerable to MS17-010
- Only in overseas cases
  - Via Dridex (Bugat v5)
  - Via CobaltStrike
  - Via Empire
  - Via Meterpreter

NLBrute

Tools for brute force using IP list, username list and password list



Servers:

Users:

Passwords:

Max attempts: 3

Thread count: 80

Timeout: 15

Default port: 3389

Good format: SERVER:PORT@DOMAIN¥USER;PASSWORD

☑ Servers checking

Statistics

Active threads: 0

Current PPS 0

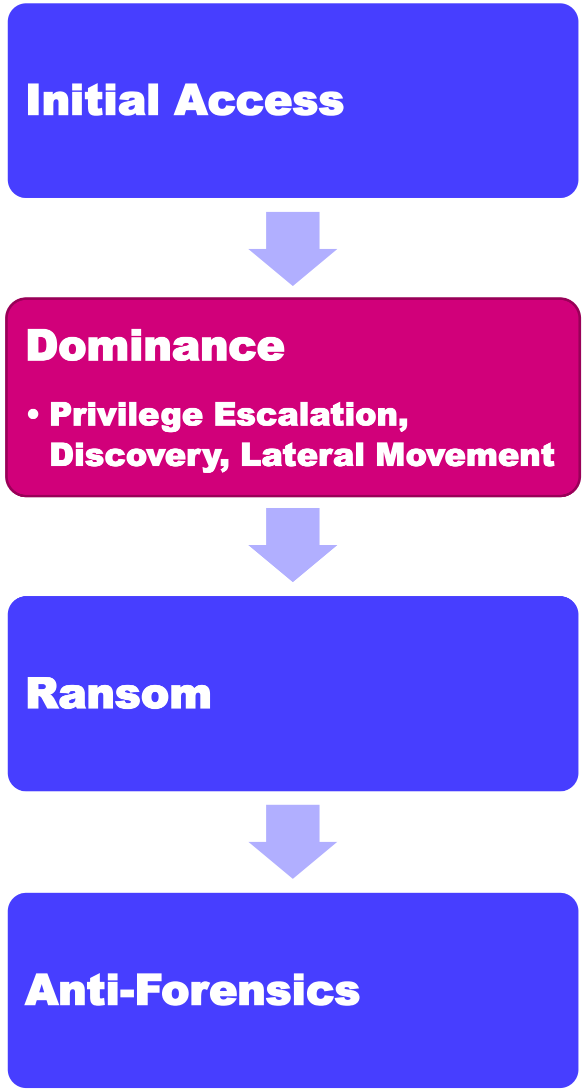
Average PPS: 0

Good count: 0

Remaining: 0

Elapsed time: 000:00:00

Privilege Escalation Techniques



Initial Access

Dominance

- Privilege Escalation, Discovery, Lateral Movement

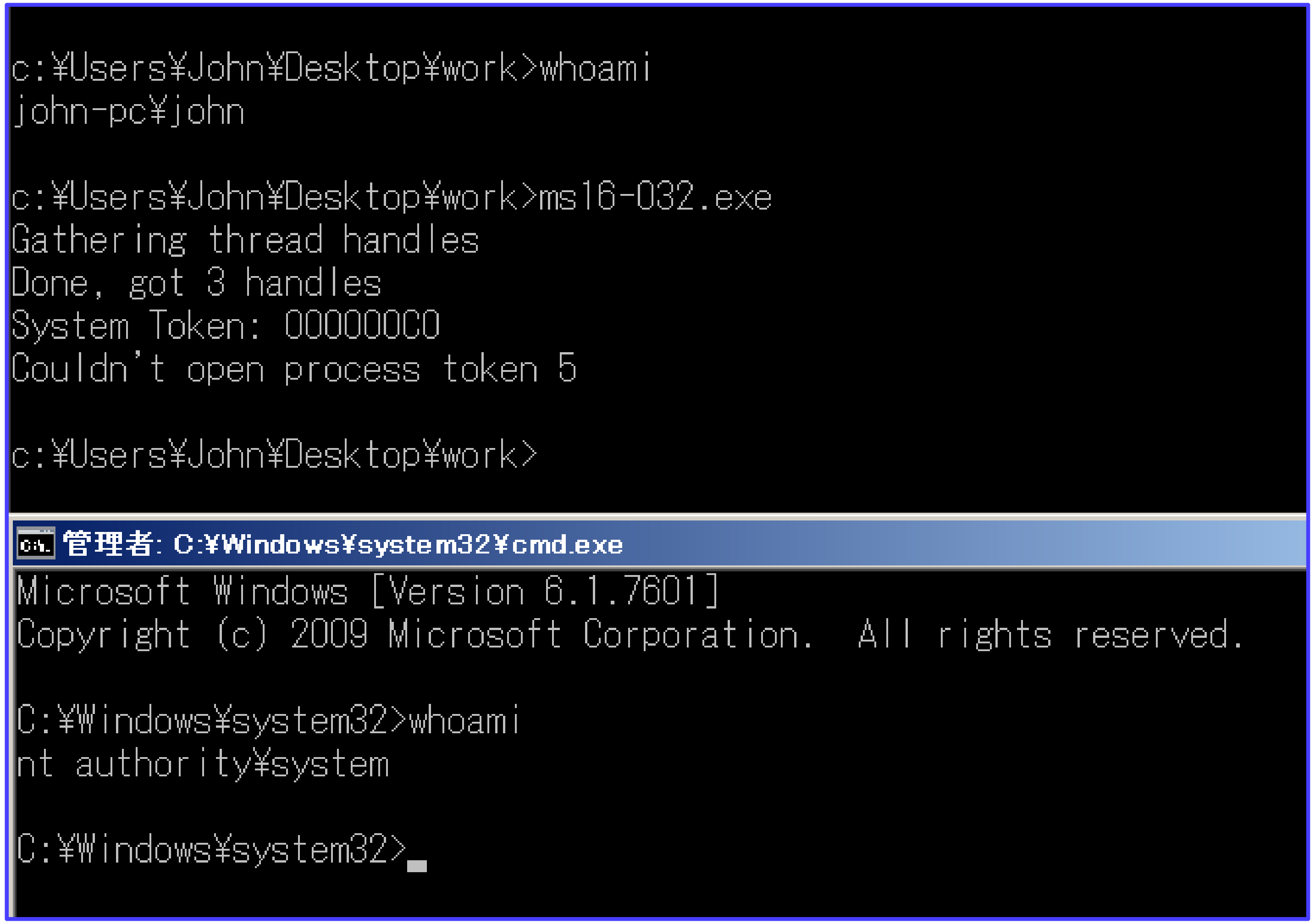
Ransom

Anti-Forensics

- Domestic and overseas cases
  - Password dump using Mimikatz
    - Executed via tools such as TrickBot and Empire
    - The account used for the intrusion is often already an administrator
- Only in domestic cases
  - Use PoC tools for specific vulnerabilities on Github

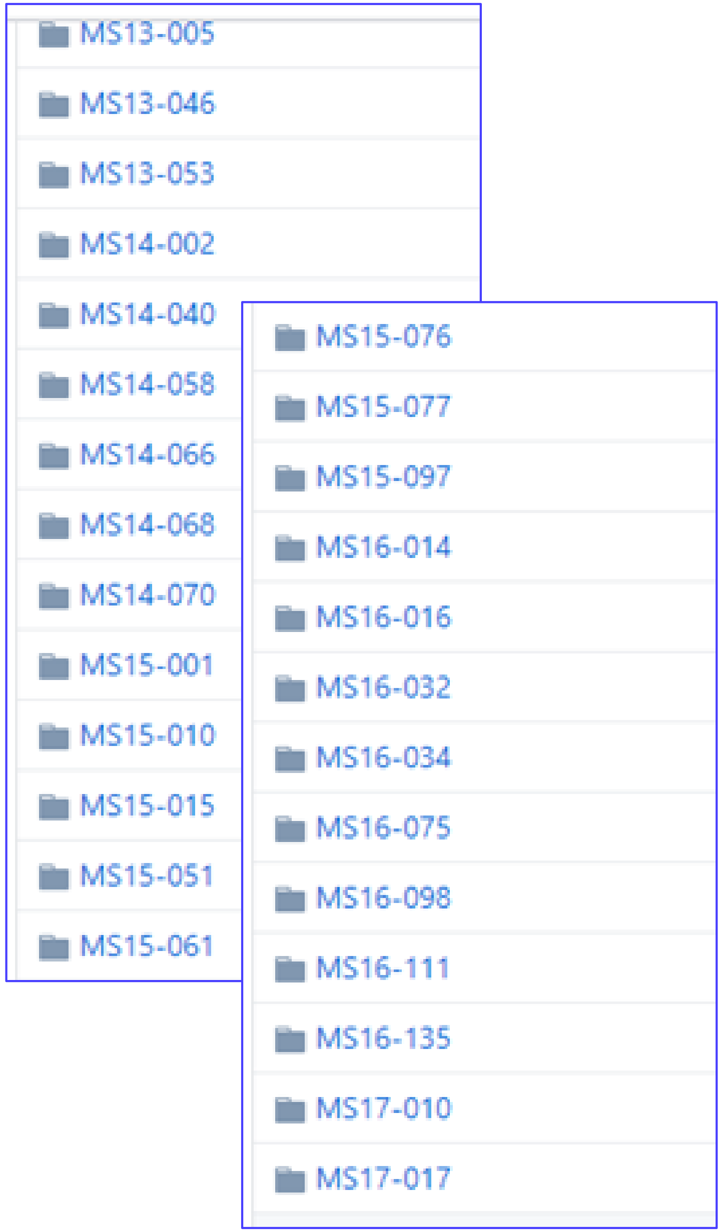
MS16-032

https://github.com/SecWiki/windows-kernel-exploits



```
c:¥Users¥John¥Desktop¥work>whoami
john-pc¥john

c:¥Users¥John¥Desktop¥work>ms16-032.exe
Gathering thread handles
Done, got 3 handles
System Token: 000000C0
Couldn't open process token 5

c:¥Users¥John¥Desktop¥work>
```

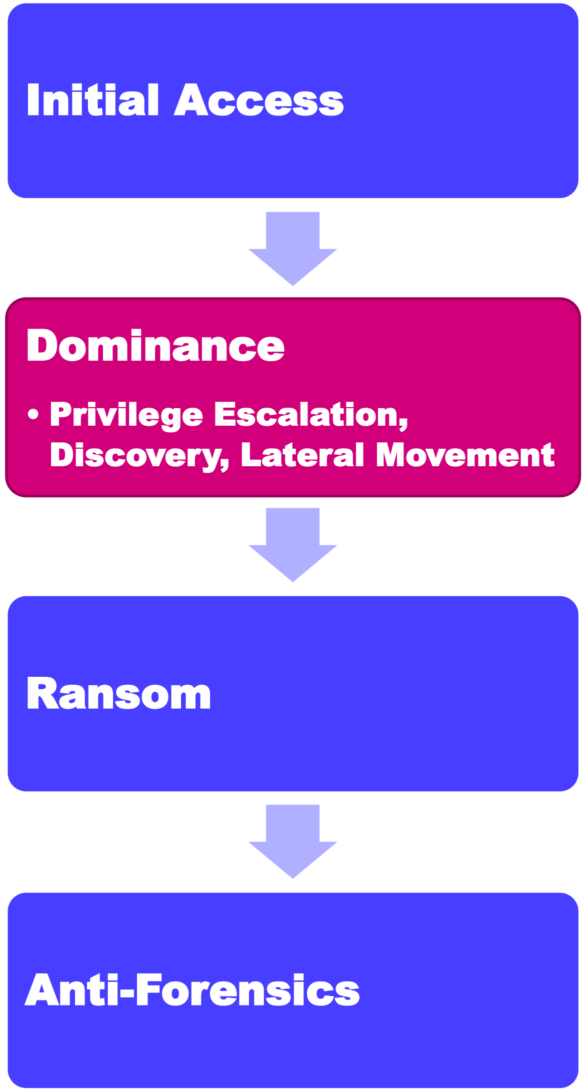
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:¥Windows¥system32>whoami
nt authority¥system

C:¥Windows¥system32>_
```



MS13-005
MS13-046
MS13-053
MS14-002
MS14-040
MS14-058
MS14-066
MS14-068
MS14-070
MS15-001
MS15-010
MS15-015
MS15-051
MS15-061

MS15-076
MS15-077
MS15-097
MS16-014
MS16-016
MS16-032
MS16-034
MS16-075
MS16-098
MS16-111
MS16-135
MS17-010
MS17-017

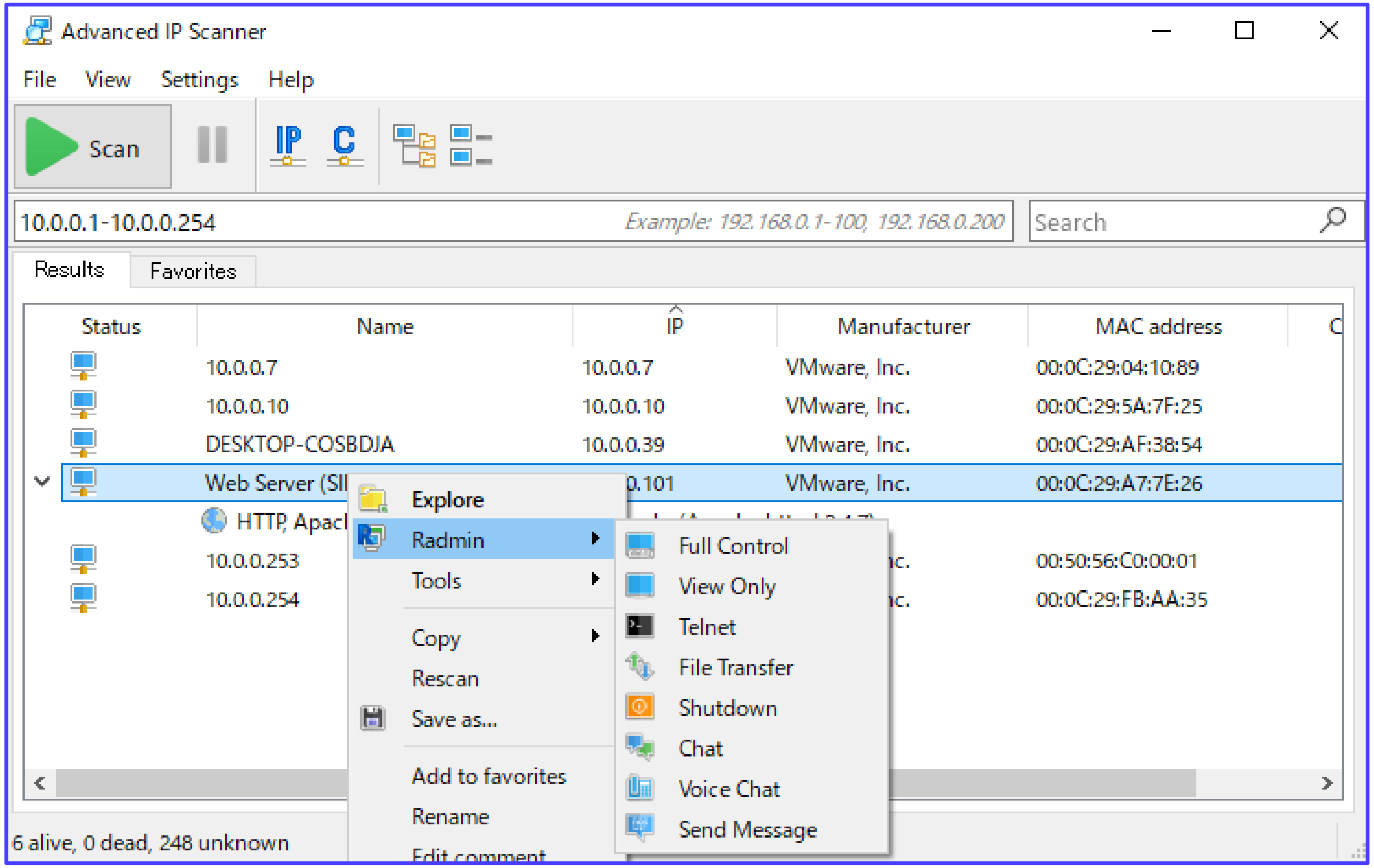
Discovery Techniques



- Domestic and overseas cases
  - Scan and gather information using malware functionality
- Only in domestic cases
  - Use Advanced IP Scanner, Advanced Port Scanner, SoftPerfect Network Scanner, ProcessHacker, KPortScan3, PowerTools, etc.
- Only in overseas cases
  - Use Hyena
  - Search AD using BloodHound and SharpHound

Advanced IP Scanner

https://www.advanced-ip-scanner.com



10.0.0.1-10.0.0.254 *Example: 192.168.0.1-100, 192.168.0.200*

Status	Name	IP	Manufacturer	MAC address	C
	10.0.0.7	10.0.0.7	VMware, Inc.	00:0C:29:04:10:89	
	10.0.0.10	10.0.0.10	VMware, Inc.	00:0C:29:5A:7F:25	
	DESKTOP-COSBDJA	10.0.0.39	VMware, Inc.	00:0C:29:AF:38:54	
	Web Server (SI	0.101	VMware, Inc.	00:0C:29:A7:7E:26	
	HTTP, Apac				
	10.0.0.253		c.	00:50:56:C0:00:01	
	10.0.0.254		c.	00:0C:29:FB:AA:35	

6 alive, 0 dead, 248 unknown

PCHunter

https://www.bleepingcomputer.com/download/pc-hunter/

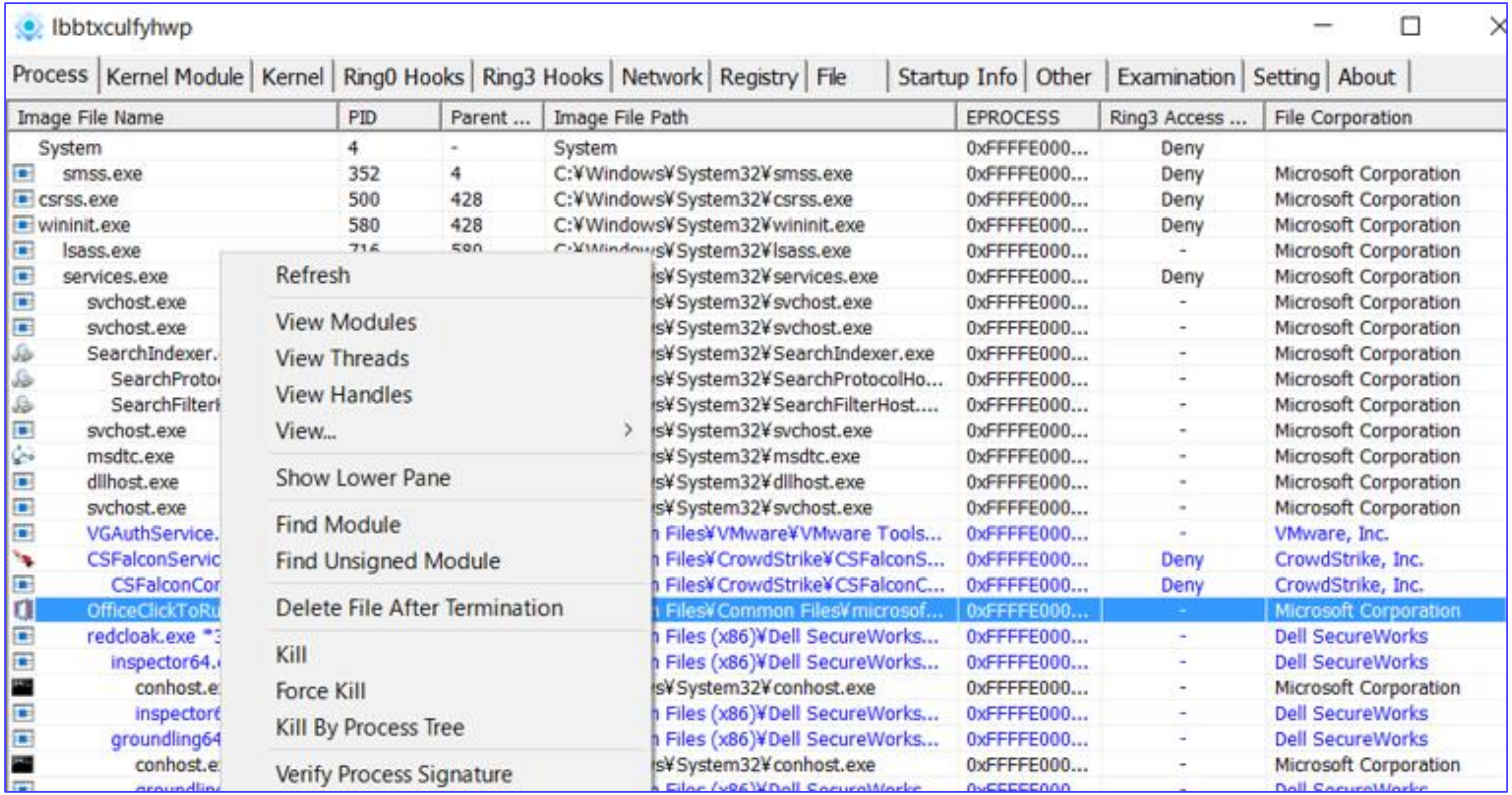
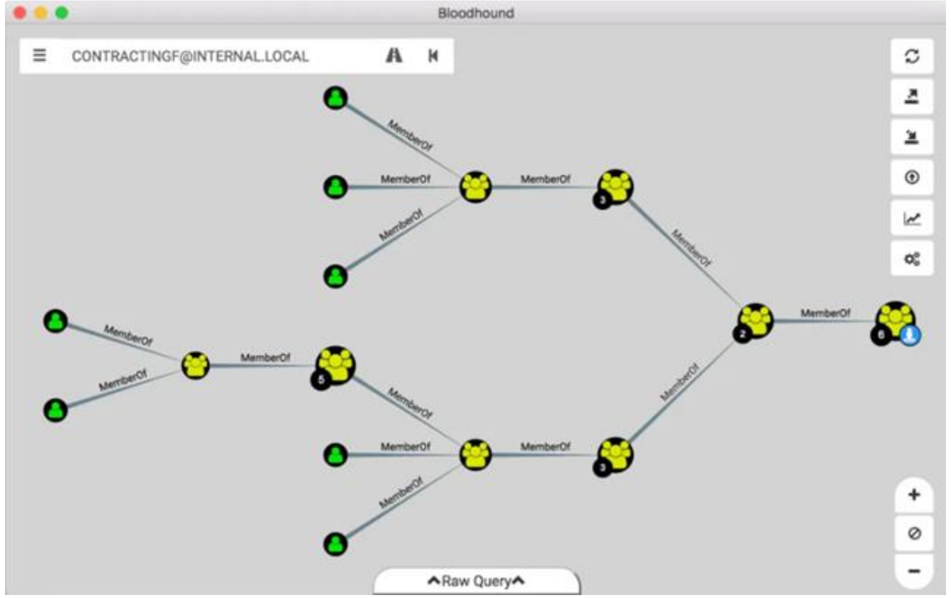


Image File Name	PID	Parent ...	Image File Path	EPROCESS	Ring3 Access ...	File Corporation
System	4	-	System	0xFFFFE000...	Deny	
smss.exe	352	4	C:¥Windows¥System32¥smss.exe	0xFFFFE000...	Deny	Microsoft Corporation
csrss.exe	500	428	C:¥Windows¥System32¥csrss.exe	0xFFFFE000...	Deny	Microsoft Corporation
wininit.exe	580	428	C:¥Windows¥System32¥wininit.exe	0xFFFFE000...	Deny	Microsoft Corporation
lsass.exe	716	580	C:¥Windows¥System32¥lsass.exe	0xFFFFE000...	-	Microsoft Corporation
services.exe			s¥System32¥services.exe	0xFFFFE000...	Deny	Microsoft Corporation
svchost.exe			s¥System32¥svchost.exe	0xFFFFE000...	-	Microsoft Corporation
svchost.exe			s¥System32¥svchost.exe	0xFFFFE000...	-	Microsoft Corporation
SearchIndexer.			s¥System32¥SearchIndexer.exe	0xFFFFE000...	-	Microsoft Corporation
SearchProto			s¥System32¥SearchProtocolHo...	0xFFFFE000...	-	Microsoft Corporation
SearchFilterI			s¥System32¥SearchFilterHost....	0xFFFFE000...	-	Microsoft Corporation
svchost.exe			s¥System32¥svchost.exe	0xFFFFE000...	-	Microsoft Corporation
msdtc.exe			s¥System32¥msdtc.exe	0xFFFFE000...	-	Microsoft Corporation
dllhost.exe			s¥System32¥dllhost.exe	0xFFFFE000...	-	Microsoft Corporation
svchost.exe			s¥System32¥svchost.exe	0xFFFFE000...	-	Microsoft Corporation
VGAuthService.			n Files¥VMware¥VMware Tools...	0xFFFFE000...	-	VMware, Inc.
CSFalconServic			n Files¥CrowdStrike¥CSFalconS...	0xFFFFE000...	Deny	CrowdStrike, Inc.
CSFalconCor			n Files¥CrowdStrike¥CSFalconC...	0xFFFFE000...	Deny	CrowdStrike, Inc.
OfficeClickToRu			n Files¥Common Files¥microsof...	0xFFFFE000...	-	Microsoft Corporation
redcloak.exe *3			n Files (x86)¥Dell SecureWorks...	0xFFFFE000...	-	Dell SecureWorks
inspector64.			n Files (x86)¥Dell SecureWorks...	0xFFFFE000...	-	Dell SecureWorks
conhost.e			s¥System32¥conhost.exe	0xFFFFE000...	-	Microsoft Corporation
inspector6			n Files (x86)¥Dell SecureWorks...	0xFFFFE000...	-	Dell SecureWorks
groundling64			n Files (x86)¥Dell SecureWorks...	0xFFFFE000...	-	Dell SecureWorks
conhost.e			s¥System32¥conhost.exe	0xFFFFE000...	-	Microsoft Corporation
groundlin			n Files (x86)¥Dell SecureWorks	0xFFFFE000	-	Dell SecureWorks

BloodHound/SharpHound

https://github.com/BloodHoundAD/BloodHound

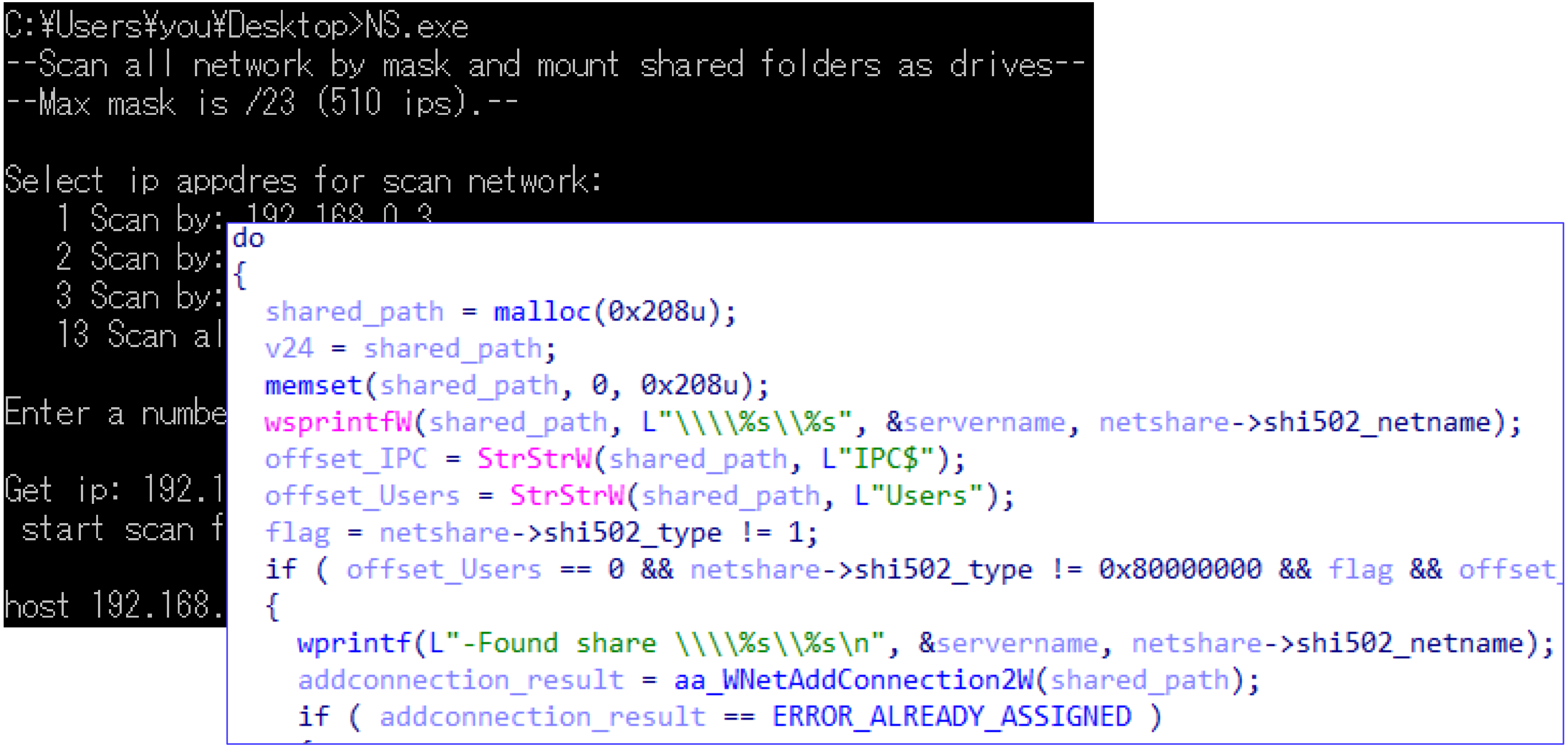
- Uncover hidden relationships and attack paths in an active directory environment
  - Aggregate various information such as usernames, computer names, groups, domains, and OUs about PCs/servers on the network and visualize their relationships
  - Identify possible attack routes to the AD server
- SharpHound is C# version of BloodHound Ingestor
  - Operate at high speed and stability



Source: https://waldo.com/?p=68

NS.exe (NetworkShare)

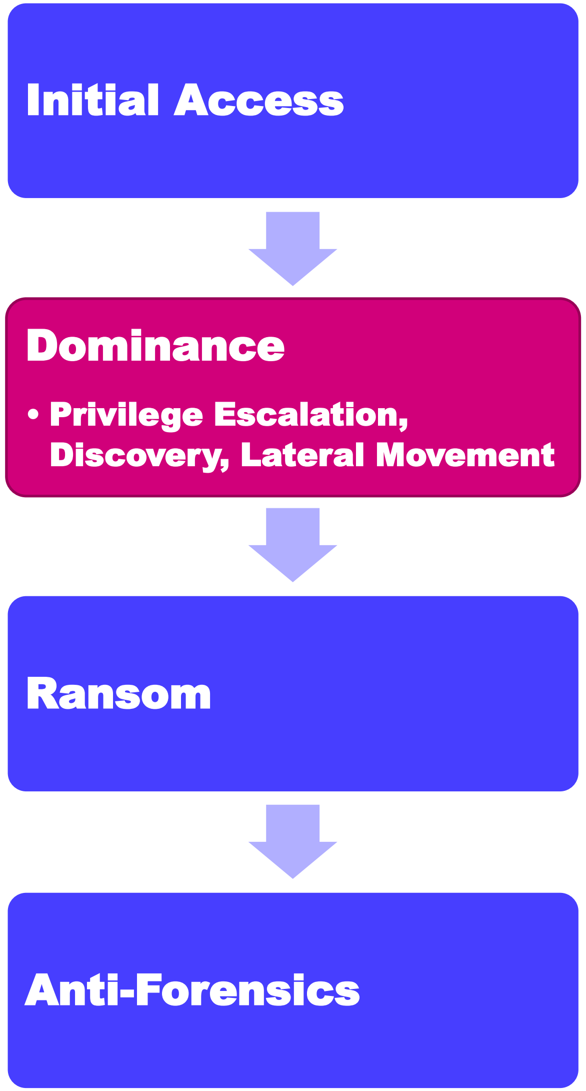
Explore network shared folders



```
C:¥Users¥you¥Desktop>NS.exe
--Scan all network by mask and mount shared folders as drives--
--Max mask is /23 (510 ips).--

Select ip appdres for scan network:
   1 Scan by: 192.168.0.3
   2 Scan by:
   3 Scan by:
   13 Scan al

Enter a numbe

Get ip: 192.1
 start scan f

host 192.168.
```

```
do
{
  shared_path = malloc(0x208u);
  v24 = shared_path;
  memset(shared_path, 0, 0x208u);
  wsprintfW(shared_path, L"\\\\%s\\%s", &servername, netshare->shi502_netname);
  offset_IPC = StrStrW(shared_path, L"IPC$");
  offset_Users = StrStrW(shared_path, L"Users");
  flag = netshare->shi502_type != 1;
  if ( offset_Users == 0 && netshare->shi502_type != 0x80000000 && flag && offset_
  {
    wprintf(L"-Found share \\\\%s\\%s\n", &servername, netshare->shi502_netname);
    addconnection_result = aa_WNetAddConnection2W(shared_path);
    if ( addconnection_result == ERROR_ALREADY_ASSIGNED )
```

Lateral Movement Techniques



Initial Access

Dominance

- Privilege Escalation, Discovery, Lateral Movement

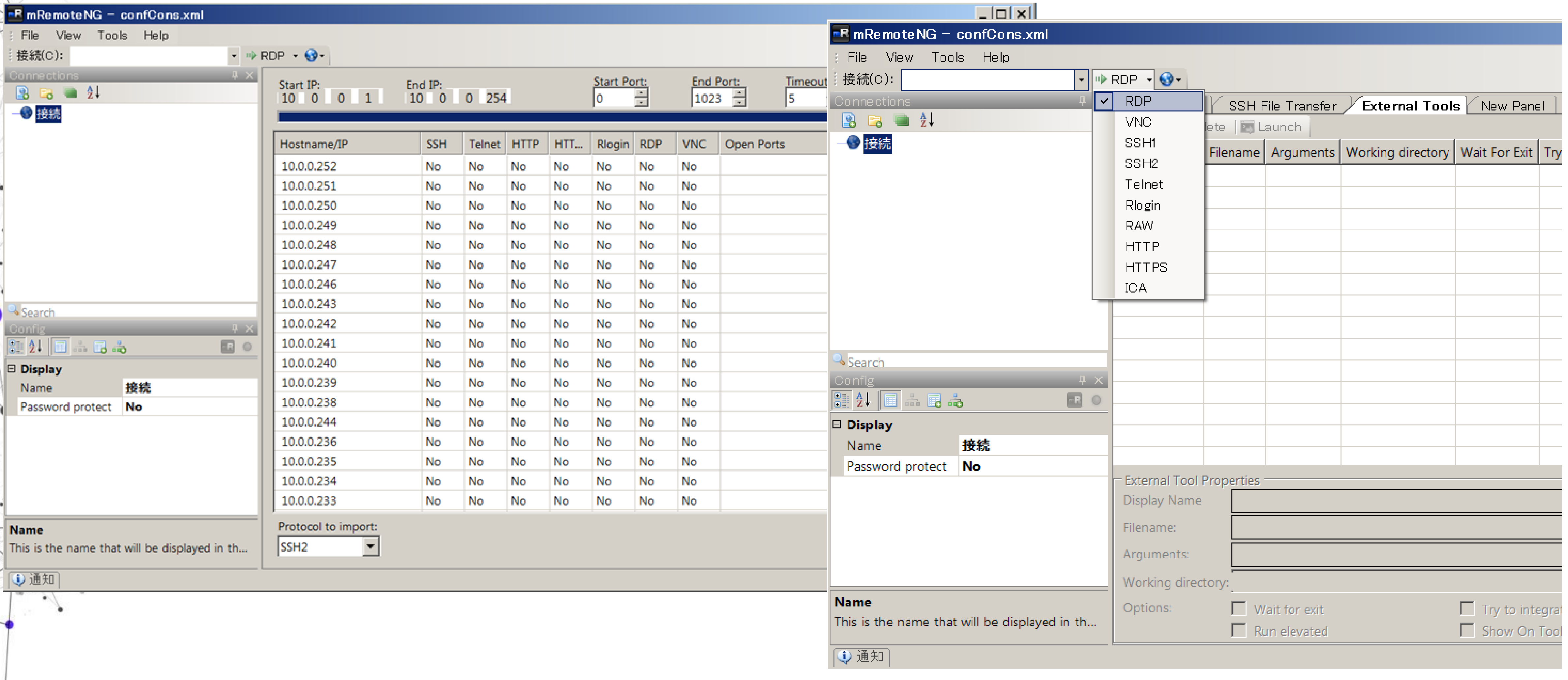
Ransom

Anti-Forensics

- Domestic and overseas cases
  - Use RDP, PsExec and WMI
- Only in domestic cases
  - Use MRemoteNG, MRemoteNC, Putty, Ammyy Admin, etc.
  - Brute-force password breach using bruttoline
- Only in overseas cases
  - Use Empire, CobaltStrike and ReGeorg

mRemoteNG

https://mremoteng.org/, https://github.com/mRemoteNG/mRemoteNG



mRemoteNG – confCons.xml

File View Tools Help

接続(C): RDP

Connections

接続

Start IP: 10 0 0 1
End IP: 10 0 0 254
Start Port: 0
End Port: 1023
Timeout: 5

Hostname/IP	SSH	Telnet	HTTP	HTT...	Rlogin	RDP	VNC	Open Ports
10.0.0.252	No	No	No	No	No	No	No	
10.0.0.251	No	No	No	No	No	No	No	
10.0.0.250	No	No	No	No	No	No	No	
10.0.0.249	No	No	No	No	No	No	No	
10.0.0.248	No	No	No	No	No	No	No	
10.0.0.247	No	No	No	No	No	No	No	
10.0.0.246	No	No	No	No	No	No	No	
10.0.0.243	No	No	No	No	No	No	No	
10.0.0.242	No	No	No	No	No	No	No	
10.0.0.241	No	No	No	No	No	No	No	
10.0.0.240	No	No	No	No	No	No	No	
10.0.0.239	No	No	No	No	No	No	No	
10.0.0.238	No	No	No	No	No	No	No	
10.0.0.244	No	No	No	No	No	No	No	
10.0.0.236	No	No	No	No	No	No	No	
10.0.0.235	No	No	No	No	No	No	No	
10.0.0.234	No	No	No	No	No	No	No	
10.0.0.233	No	No	No	No	No	No	No	

Protocol to import: SSH2

Search

Config

Display

Name	接続
Password protect	No

Name

This is the name that will be displayed in th...

通知

mRemoteNG – confCons.xml

File View Tools Help

接続(C): RDP

SSH File Transfer | External Tools | New Panel

ete | Launch

Filename	Arguments	Working directory	Wait For Exit	Try

Connections

接続

Search

Config

Display

Name	接続
Password protect	No

Name

This is the name that will be displayed in th...

通知

External Tool Properties

Display Name:

Filename:

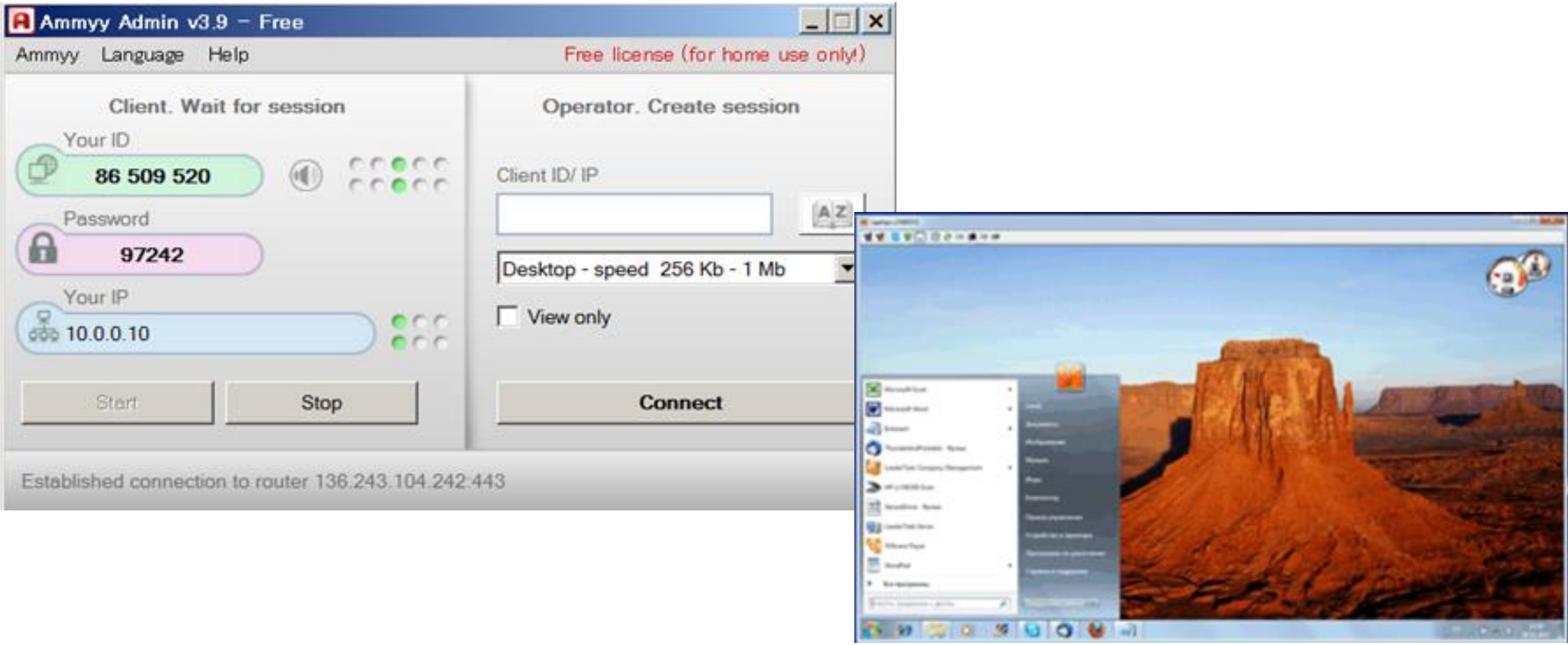
Arguments:

Working directory:

Options: □ Wait for exit □ Try to integra
□ Run elevated □ Show On Tool

Ammyy Admin

http://www.ammyy.com/en/



Ammyy Admin v3.9 – Free

Ammyy Language Help

Free license (for home use only!)

Client. Wait for session

Your ID: 86 509 520

Password: 97242

Your IP: 10.0.0.10

Start | Stop

Operator. Create session

Client ID/ IP:

Desktop - speed 256 Kb - 1 Mb

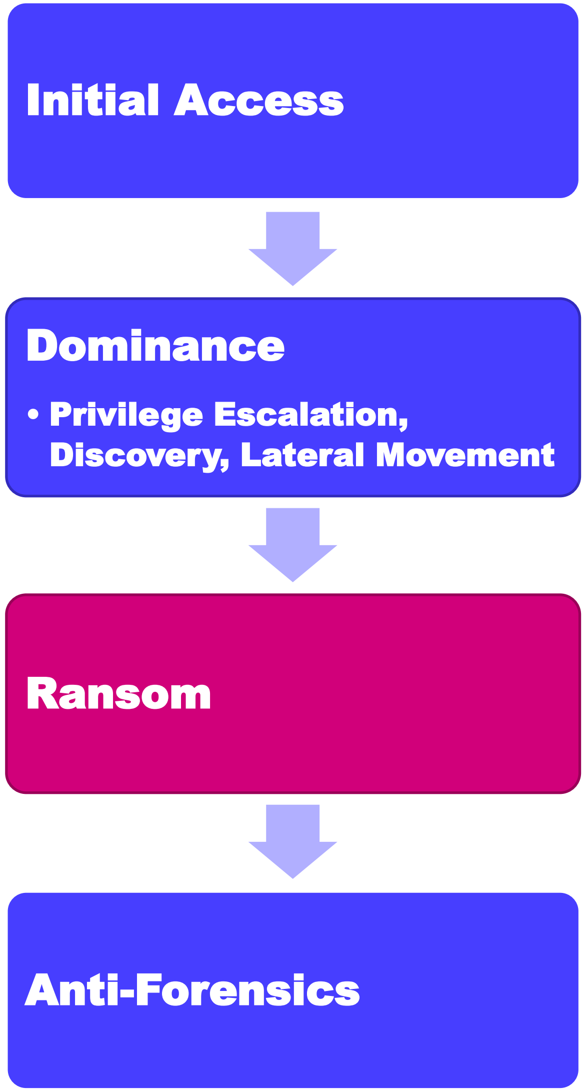
□ View only

Connect

Established connection to router 136.243.104.242:443

Source: http://www.ammyy.com/en/admin_screenshots.html

Ransom Techniques



Initial Access

Dominance

- Privilege Escalation, Discovery, Lateral Movement

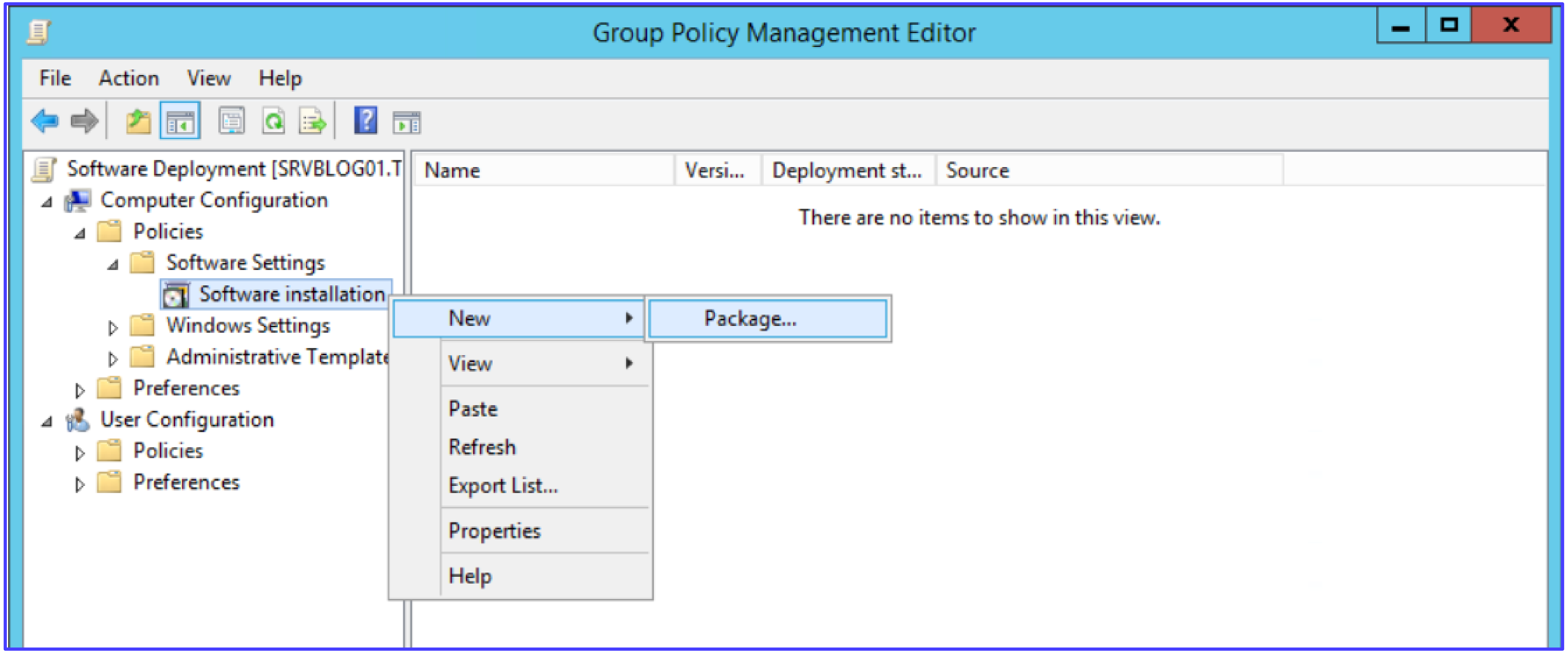
Ransom

Anti-Forensics

- Domestic and overseas cases
  - Run ransomware using PsExec, RDP and WMI
  - Deploy and execute ransomware using RAT and post-exploitation framework function
  - Use batch files or powershell scripts
  - Distribute ransomware using group policy function (software installation and logon scripts) via AD server
  - Use various families of ransomware

Ransomware Distribution from AD Server

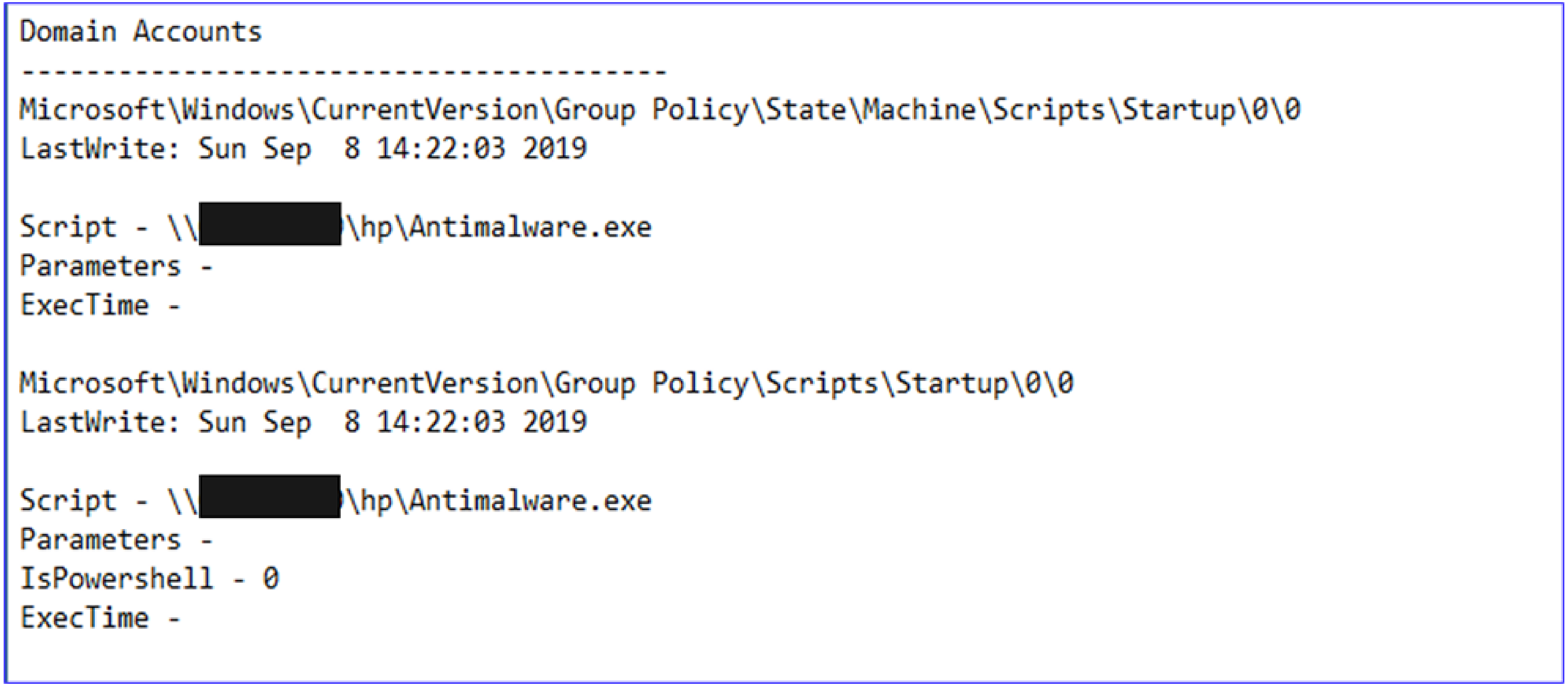
Use "Software installation" to broadcast ransomware



There are no items to show in this view.

Ransomware Distribution from AD Server

Use “Logon Script” to broadcast ransomware



```
Domain Accounts
----------------------------------------
Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Scripts\Startup\0\0
LastWrite: Sun Sep  8 14:22:03 2019

Script - \\[redacted]\hp\Antimalware.exe
Parameters -
ExecTime -

Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup\0\0
LastWrite: Sun Sep  8 14:22:03 2019

Script - \\[redacted]\hp\Antimalware.exe
Parameters -
IsPowershell - 0
ExecTime -
```

Types of Ransomware

- Matrix
- Phobos
- GandCrab
- GlobeImposter
- Cropp
- Dharma
- Ryuk
- MedusaLocker
- Frendi
- CrySiS
- Scarab
- Samsam
- BitPaymer
- Defray 777
- REvil/Sodinokibi
- rsa.exe/aes.exe

Typical Features of Ransomware

File encryption

- Use in combination with RSA-2048/RSA-4096 and AES-256
- Encrypt file data with AES, which allows high-speed encryption. Then, the used AES secret key is encrypted with the RSA public key

Scan the network and add more PCs/servers to encrypt

- Explore A-Z drives
- Explore network shared folders, administrative shares, etc.
- Disable firewall

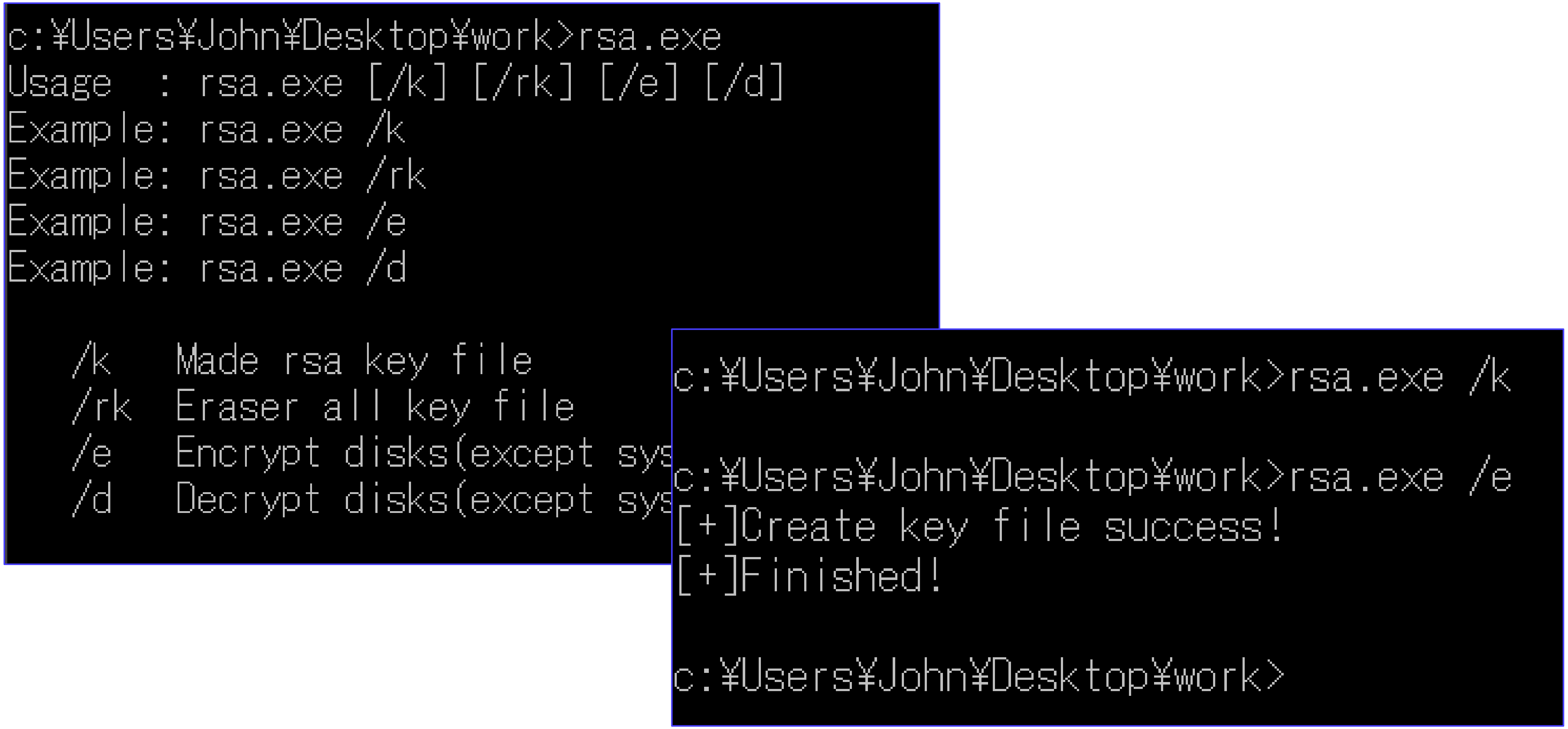
Anti-forensics

- Erase VSS
- Disable startup repair

Display ransom note

Command Line Tools “rsa.exe”

Ransomware but closer to an encryption tool

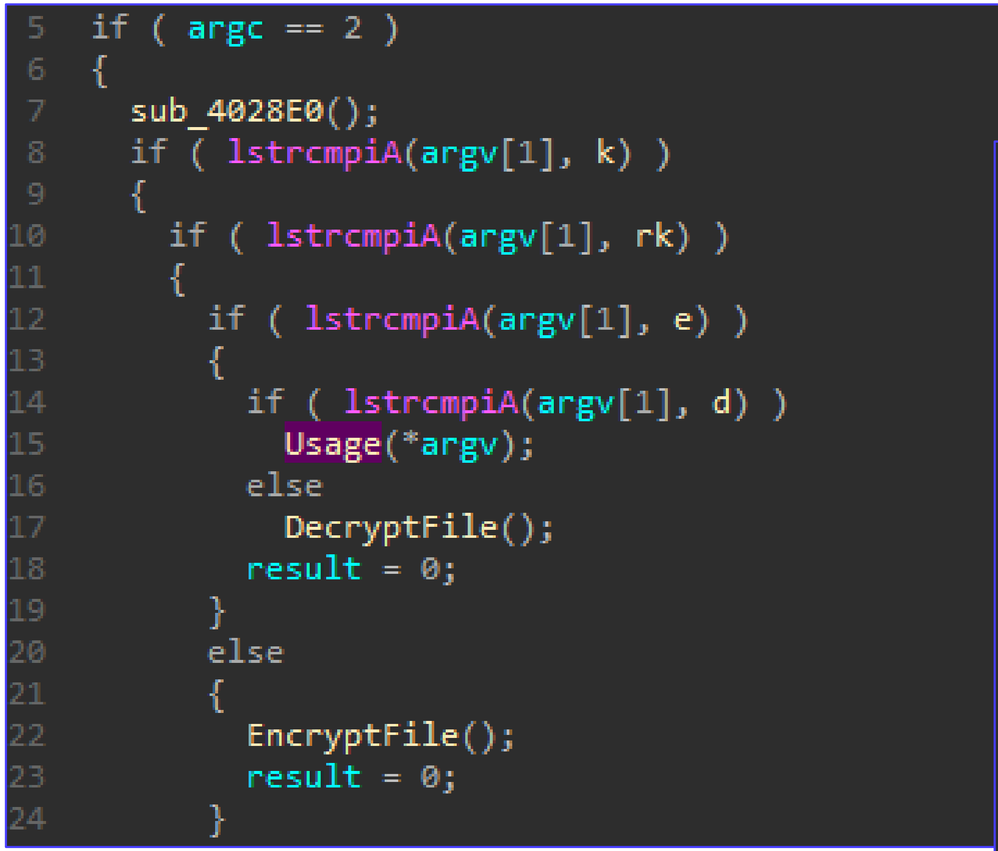


```
c:¥Users¥John¥Desktop¥work>rsa.exe
Usage  : rsa.exe [/k] [/rk] [/e] [/d]
Example: rsa.exe /k
Example: rsa.exe /rk
Example: rsa.exe /e
Example: rsa.exe /d

   /k   Made rsa key file
   /rk  Eraser all key file
   /e   Encrypt disks(except sys
   /d   Decrypt disks(except sys
```

```
c:¥Users¥John¥Desktop¥work>rsa.exe /k

c:¥Users¥John¥Desktop¥work>rsa.exe /e
[+]Create key file success!
[+]Finished!

c:¥Users¥John¥Desktop¥work>
```

Command Line Tools “rsa.exe”

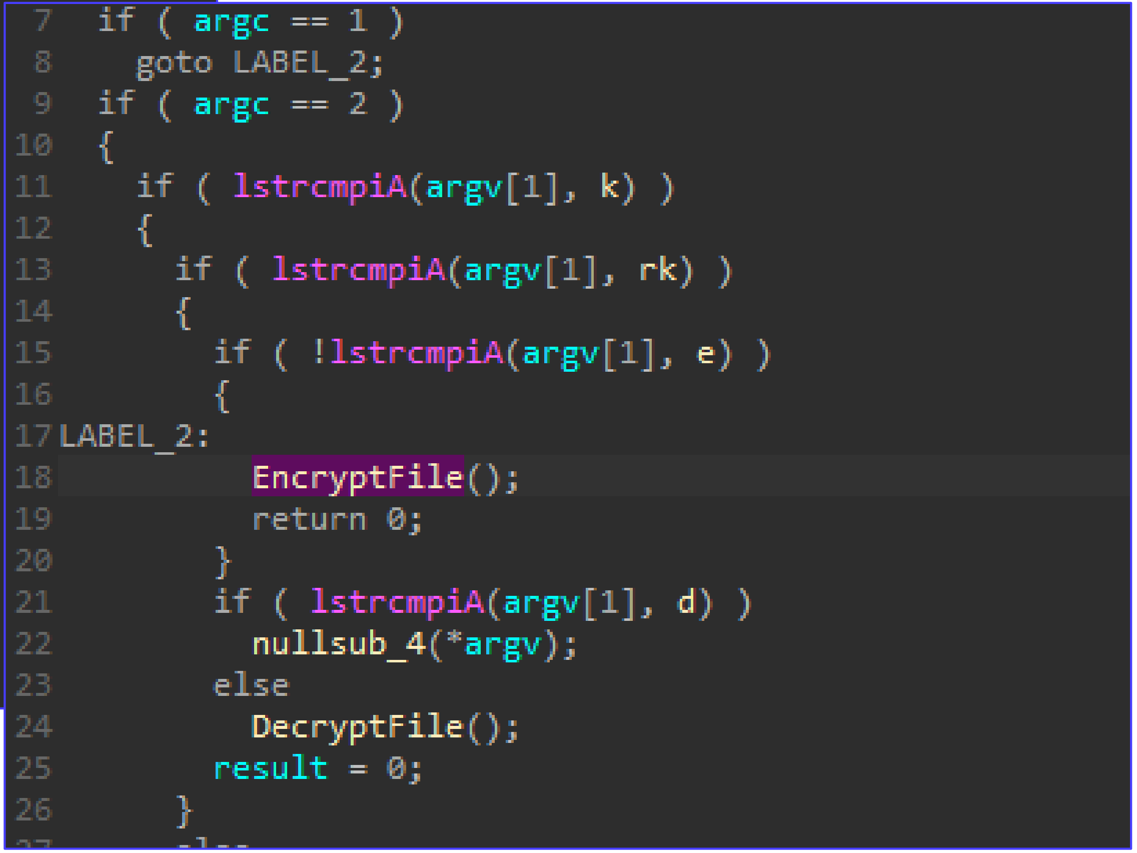
Confirm multiple versions



```
if ( argc == 2 )
{
  sub_4028E0();
  if ( lstrcmpiA(argv[1], k) )
  {
    if ( lstrcmpiA(argv[1], rk) )
    {
      if ( lstrcmpiA(argv[1], e) )
      {
        if ( lstrcmpiA(argv[1], d) )
          Usage(*argv);
        else
          DecryptFile();
        result = 0;
      }
      else
      {
        EncryptFile();
        result = 0;
      }
```

Usage version

No usage version
(Encrypt file if there is no arguments)



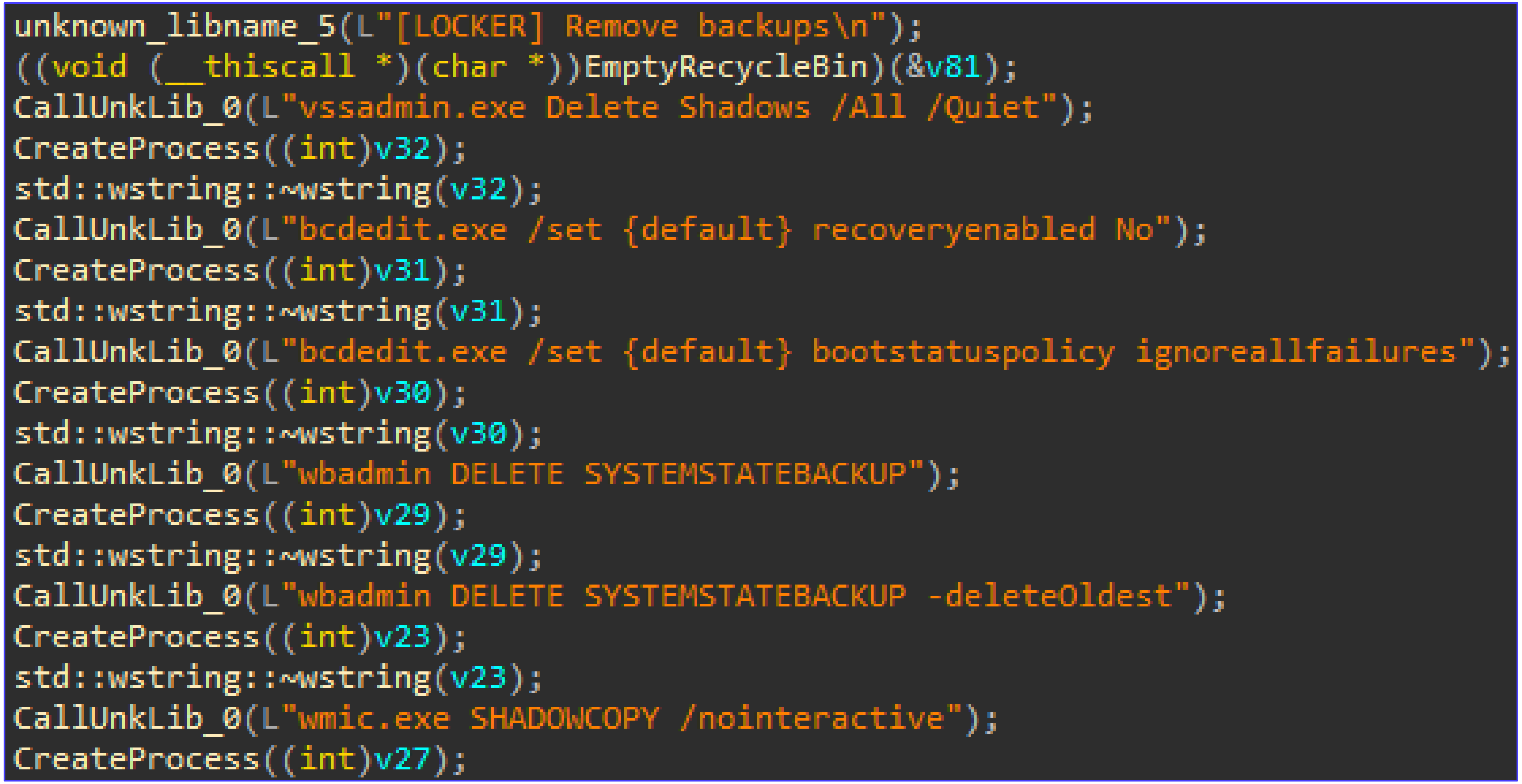
```
if ( argc == 1 )
  goto LABEL_2;
if ( argc == 2 )
{
  if ( lstrcmpiA(argv[1], k) )
  {
    if ( lstrcmpiA(argv[1], rk) )
    {
      if ( !lstrcmpiA(argv[1], e) )
      {
LABEL_2:
        EncryptFile();
        return 0;
      }
      if ( lstrcmpiA(argv[1], d) )
        nullsub_4(*argv);
      else
        DecryptFile();
      result = 0;
    }
    else
```

Command Examples

- Spread of infection
  - "netsh advfirewall set currentprofile state off"
  - "netsh firewall set opmode mode=disable”
- Anti-forensics
  - "wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0"
  - "vssadmin delete shadows /all /quiet"
  - "wmic shadowcopy delete /nointeractive"
  - "bcdedit /set {default} bootstatuspolicy ignoreallfailures"
  - "bcdedit /set {default} recoveryenabled no”
  - "C:¥Windows¥system32¥cmd.exe“ /c del <malware execution path>¥<malware name> > nul

Commands Hard-Coded into the Ransomware

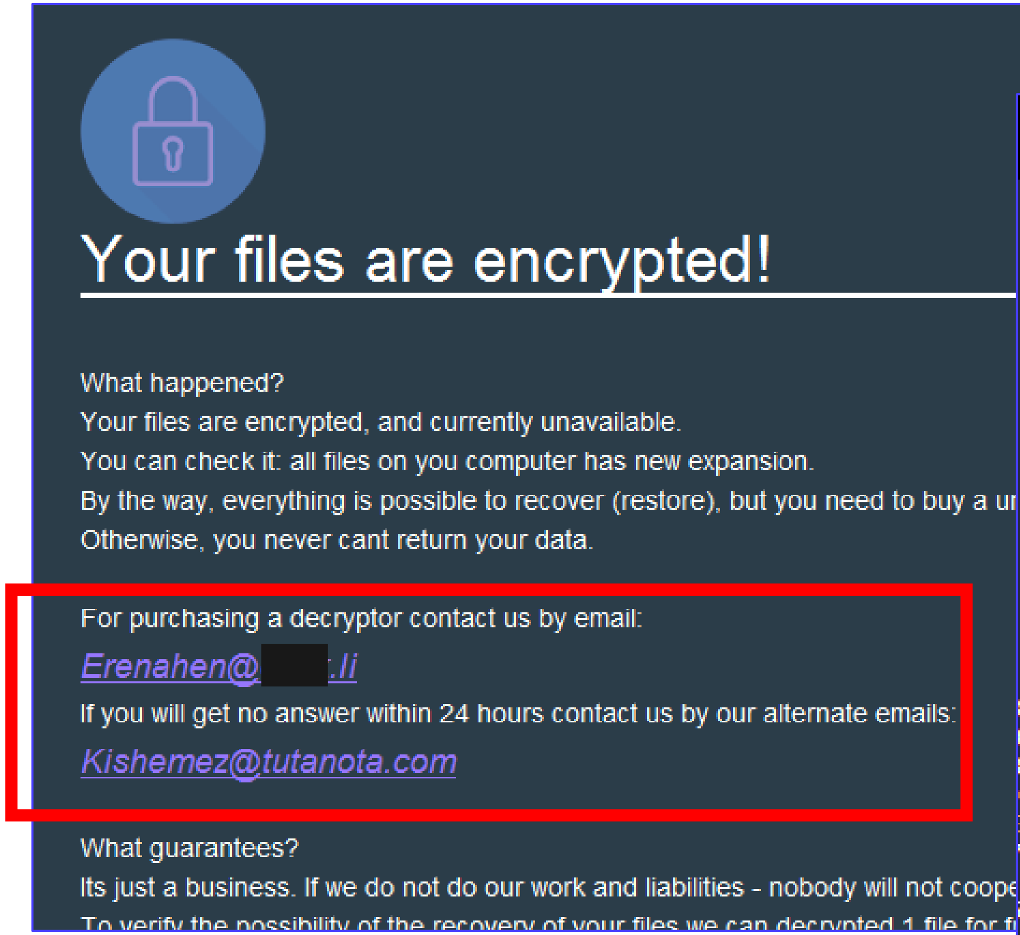
MedusaLocker



```
unknown_libname_5(L"[LOCKER] Remove backups\n");
((void (__thiscall *)(char *))EmptyRecycleBin)(&v81);
CallUnkLib_0(L"vssadmin.exe Delete Shadows /All /Quiet");
CreateProcess((int)v32);
std::wstring::~wstring(v32);
CallUnkLib_0(L"bcdedit.exe /set {default} recoveryenabled No");
CreateProcess((int)v31);
std::wstring::~wstring(v31);
CallUnkLib_0(L"bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures");
CreateProcess((int)v30);
std::wstring::~wstring(v30);
CallUnkLib_0(L"wbadmin DELETE SYSTEMSTATEBACKUP");
CreateProcess((int)v29);
std::wstring::~wstring(v29);
CallUnkLib_0(L"wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest");
CreateProcess((int)v23);
std::wstring::~wstring(v23);
CallUnkLib_0(L"wmic.exe SHADOWCOPY /nointeractive");
CreateProcess((int)v27);
```

Ransom Note Trends

Instead of Bitcoin transfers, attacker requires direct email contact

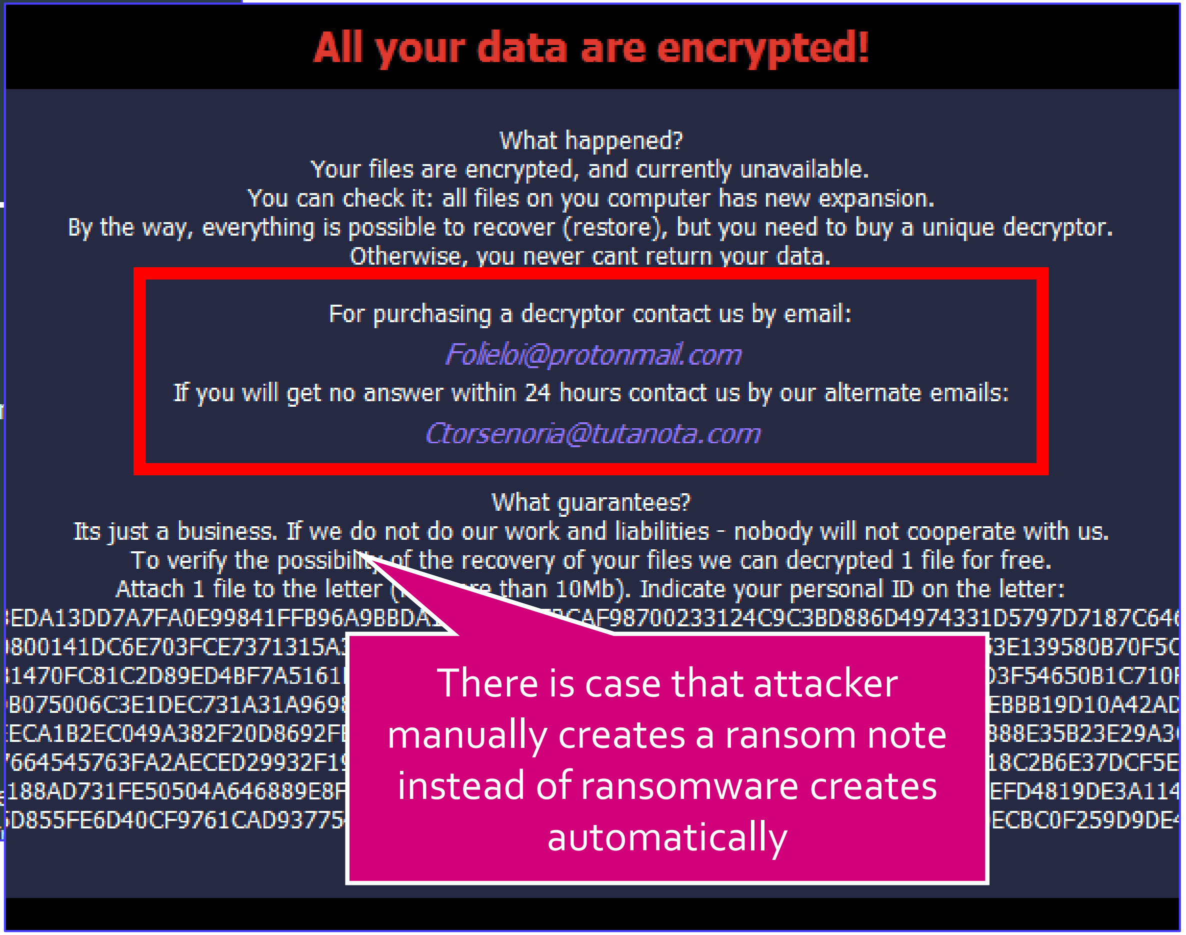


Your files are encrypted!

What happened?
Your files are encrypted, and currently unavailable.
You can check it: all files on you computer has new expansion.
By the way, everything is possible to recover (restore), but you need to buy a ur
Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:
Erenahen@[redacted].li
If you will get no answer within 24 hours contact us by our alternate emails:
Kishemez@tutanota.com

What guarantees?
Its just a business. If we do not do our work and liabilities - nobody will not coope
To verify the possibility of the recovery of your files we can decrypted 1 file for fr



All your data are encrypted!

What happened?
Your files are encrypted, and currently unavailable.
You can check it: all files on you computer has new expansion.
By the way, everything is possible to recover (restore), but you need to buy a unique decryptor.
Otherwise, you never cant return your data.

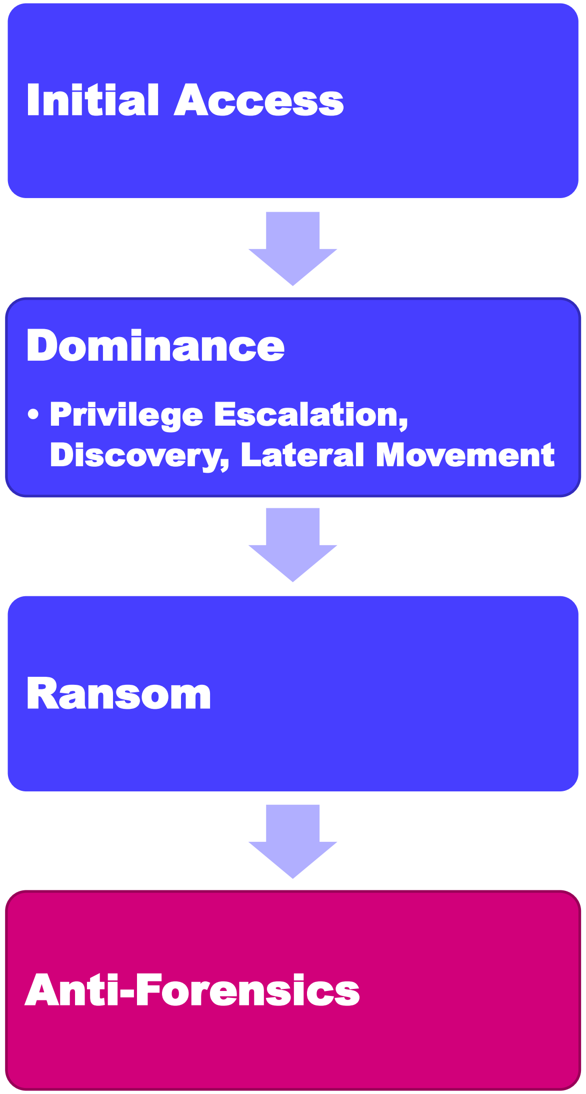
For purchasing a decryptor contact us by email:
Folieloi@protonmail.com
If you will get no answer within 24 hours contact us by our alternate emails:
Ctorsenoria@tutanota.com

What guarantees?
Its just a business. If we do not do our work and liabilities - nobody will not cooperate with us.
To verify the possibility of the recovery of your files we can decrypted 1 file for free.
Attach 1 file to the letter (n re than 10Mb). Indicate your personal ID on the letter:

```
EDA13DD7A7FA0E99841FFB96A9BBDA1         CAF98700233124C9C3BD886D4974331D5797D7187C646
800141DC6E703FCE7371315A3                                     3E139580B70F5C
1470FC81C2D89ED4BF7A5161                                      03F54650B1C710F
B075006C3E1DEC731A31A9698                                     EBBB19D10A42AD
ECA1B2EC049A382F20D8692FE                                     888E35B23E29A3
664545763FA2AECED29932F19                                     18C2B6E37DCF5E
188AD731FE50504A646889E8F                                     EFD4819DE3A114
D855FE6D40CF9761CAD93775                                      ECBC0F259D9DE
```

There is case that attacker manually creates a ransom note instead of ransomware creates automatically

Anti-Forensics Techniques



Initial Access

Dominance

- Privilege Escalation, Discovery, Lateral Movement

Ransom

Anti-Forensics

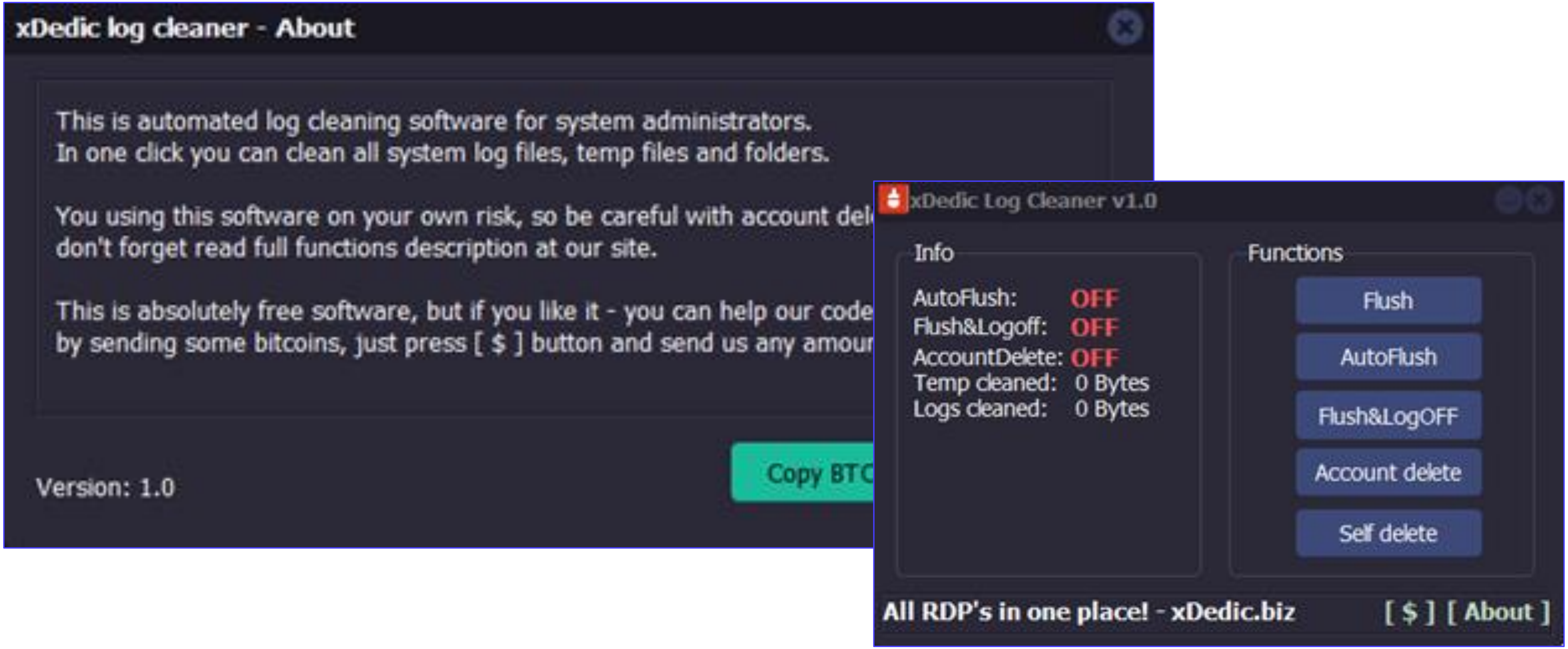
- Domestic and overseas cases
  - Erase VSS, disable FW using ransomware
  - Delete file using “sdelete.exe –p 5 <FileName>”
  - Delete eventlog using “pslog.exe -c security”, etc.
  - There are many cases in which evidence deletion has not been carried out both domestic and overseas
  - Some evidence is erased because ransomware encrypts registry, eventlog and other files
- Only in domestic cases
  - Use xDedicLogCleaner

Uninstalling Security Products Using PowerShell

- Execution history
  - C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥PowerShell ¥PSReadline¥ConsoleHost_history.txt
- Commands
  - (Get-WmiObject -Class Win 32_Product -Filter "Name = 'Symantec Endpoint Protection'" - ComputerName.).Uninstall()
  - (Get-WmiObject -Class Win 32_Product -Filter "Name = 'Endpoint Protection'" - ComputerName.).Uninstall()

xDedicLogCleaner

One click to clear various PC history



xDedic log cleaner - About

This is automated log cleaning software for system administrators.
In one click you can clean all system log files, temp files and folders.

You using this software on your own risk, so be careful with account del
don't forget read full functions description at our site.

This is absolutely free software, but if you like it - you can help our code
by sending some bitcoins, just press [$] button and send us any amour

Version: 1.0

xDedic Log Cleaner v1.0

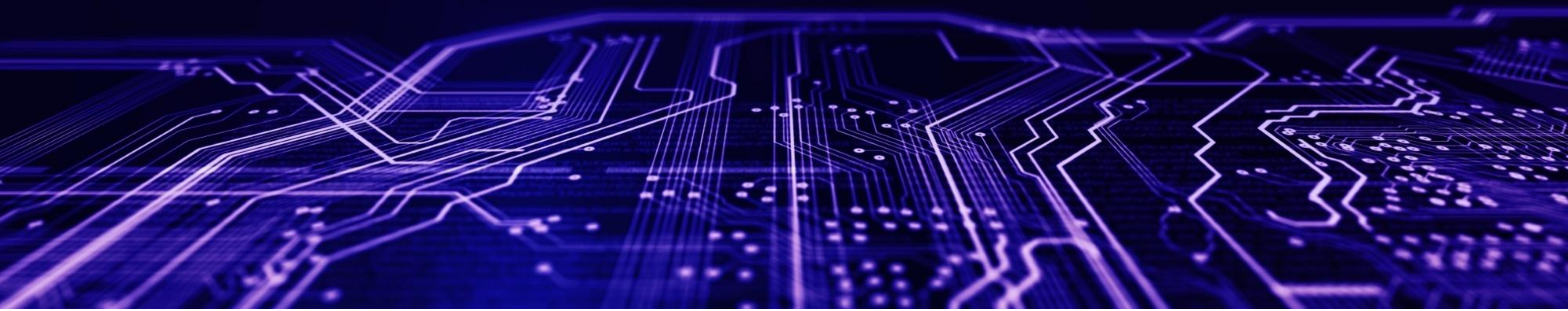
Info

AutoFlush: OFF
Flush&Logoff: OFF
AccountDelete: OFF
Temp cleaned: 0 Bytes
Logs cleaned: 0 Bytes

All RDP's in one place! - xDedic.biz

Comparison with Targeted Attacks

Results of Targeted Ransomware Incident Investigations



TTPs in Each Case

TTPs differs depending on the case

	Initial Access	Dominance	Ransom	Evidence Deletion
Domestic and Overseas 1	Mail (Emotet)	TrickBot	Ryuk	N/A
Domestic 2	RDP	MS16 -032, NLBrute, Advanced IP Scanner, AmmyAdmin, NetworkShare.exe	Matrix	N/A
Domestic 3	RDP	Advanced Port Scanner, ProcessHacker NetworkShare.exe	Phobos	N/A
Domestic 4	RDP	PCHunter, ProcessHacker, Mimikatz	Phobos	N/A
Domestic 5	RDP	KPortScan3, SoftPerfectNetworkScanner, Powertools, mRemoteNG, Bruttoline, Putty, ProcessHacker, Mimikatz	GandCrab	xDedicLogCleaner
Domestic 6	VPN	PsExec Batch file about DomainUser listing	rsa.exe	pslog.exe sdelete.exe
Domestic 7	RDP	PsExec	GlobeImposter 2.0	N/A
Overseas 2	RDP	Hyena, Mimikatz, WMIexec, reGeorg	Samsam	N/A
Overseas 3	Mail (Dridex)	Empire, PsExec	BitPaymer	N/A
Overseas 4	Mail	CobaltStrike, Meterpreter, SharpHound	Defray 777	N/A

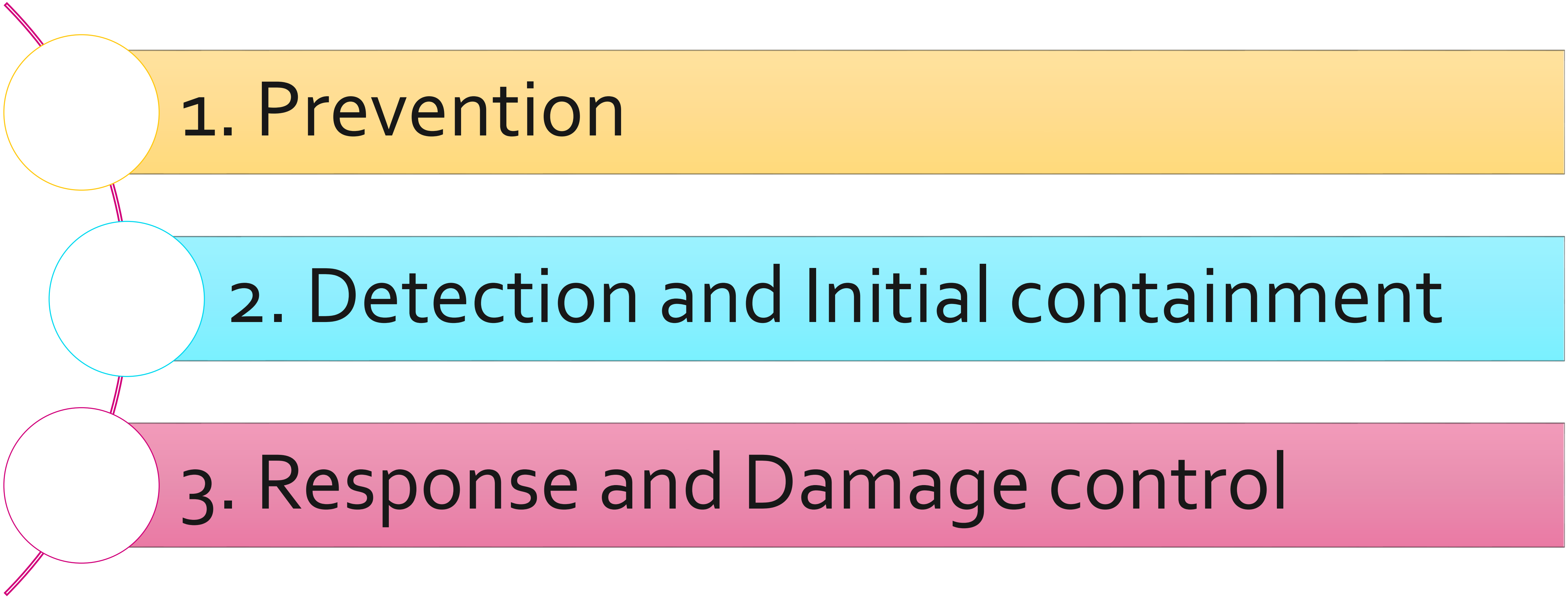
Characteristics Unique to Targeted Ransomware Attacks

- Attempt to break into various organizations and attack targets with weak security measures and easy ransomware deployment
- Heavily use brute force when attacker cracks password
- Heavily use free tools when attacker dominates systems
- Use AD server’s group policies function (software installation and logon scripts)
- Ransomware type/version used by the attacker changes quickly
- Many overseas cases are similar to TTPs for targeted attacks (penetration test)

Fight Against Targeted Ransomware Incidents

Preparation

Prepare countermeasures and response plans from the following perspectives



1. Prevention
2. Detection and Initial containment
3. Response and Damage control

1. Prevention

- Implement countermeasures to prevent “Initial Access” “Dominance" and “Ransom" to increase the cost of successful attacks
  - Unlike targeted attacks, attacker aims organization with poor security.

Prevent “Initial Access"

- FW (Network, Personal, Security Group for Cloud, etc.)
- Vulnerability Management for VPNs and Other Network Devices
- E-Mail Security
- Anti-virus

Prevent “Dominance"

- Network Segmentation and Access Control
- Application whitelists, etc.
- Appropriate management of Local and Domain administrative accounts
- Domain Controller Protection

Prevent “Ransom"

- Appropriate data access restrictions(Least privilege principle)
- Acquire backup and store Ransomware-safely
- Implement advanced endpoint security which can detect and protect against file encryption

2. Detection and Initial containment

- In most incidents, existing security products can detect something signs of attacks.
    - Unlike targeted attacks, attacks are less stealthy
- However, requires quick initial containment to minimize damage.
    - Initial containment planning is essential for quick response.

Monitoring security alerts

- Anti-virus
- EDR
- Mail
- Malicious usage of administrative accounts
- VPN

Identify threat type and severity

- Identify type of malware and attack tools.
- Malicious Usage of high-privilege accounts
- Any activities related to "Dominance"

Initial containment planning

- Isolation of affected computers
- Cut off corporate networks as a precaution
- Cut off all Internet access as a precaution
- Resetting passwords for all administrative account as a precaution

3. Response and Damage control

- Recovery plan is required to quickly recover encrypted data and minimize business impact.
  - Just acquire backup is not enough for practical recovery
- Investigation, containment, and eradication processes must be planned in advance like targeted attacks.

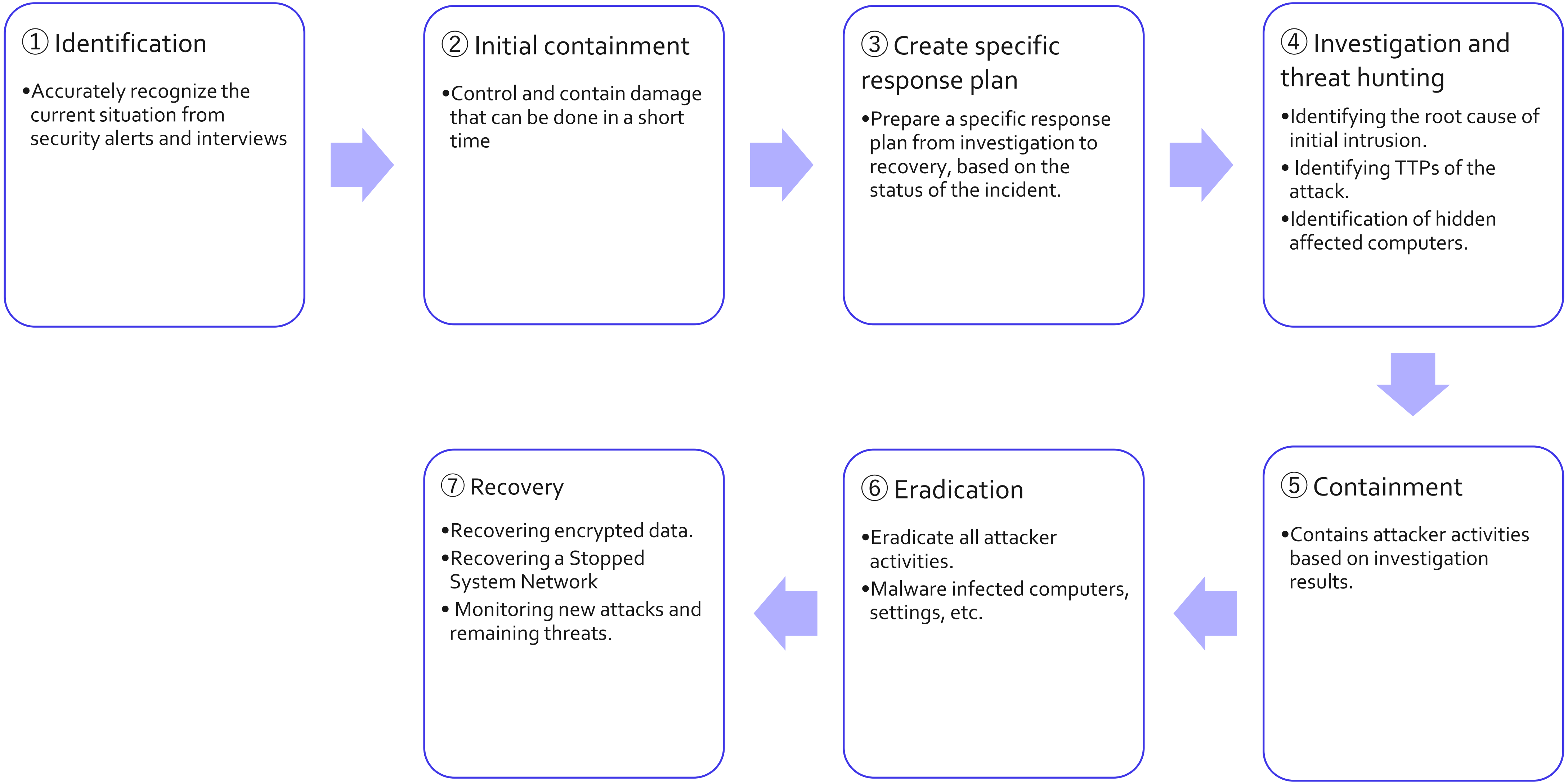
Recovery plan after encryption

- System Recovery Priority
- Recovery time objectives
- Prepare a cold standby system for most critical systems
- Manpower and procedures for carrying out restoration

"investigation" "containment" and "eradication" plans

- Manpower, Operation, and Costs
- Target response time
- Targets to be achieved at each stage of incident response process
- Preparation of specific tasks and procedures of each stage of incident response process

Incident Response Process and Points



① Identification

- Accurately recognize the current situation from security alerts and interviews

② Initial containment

- Control and contain damage that can be done in a short time

③ Create specific response plan

- Prepare a specific response plan from investigation to recovery, based on the status of the incident.

④ Investigation and threat hunting

- Identifying the root cause of initial intrusion.
- Identifying TTPs of the attack.
- Identification of hidden affected computers.

⑤ Containment

- Contains attacker activities based on investigation results.

⑥ Eradication

- Eradicate all attacker activities.
- Malware infected computers, settings, etc.

⑦ Recovery

- Recovering encrypted data.
- Recovering a Stopped System Network
- Monitoring new attacks and remaining threats.

Balance between Business and Safety

- System recovery is often a priority because data encryption means business disruption
- In some cases, the previous incident response process cannot be performed step by step.
- A response plan that balances business continuity and safety needs to be developed within a limited time frame
- What should be kept to a minimum to prevent the recurrence of attacks and the spread of damage?

Examples of incidents and responses in Japan and overseas should be widely shared with incident handlers, in order to create
best practices is especially important for quick, safe incident response and minimize business Impact

Important points for preventing damage expansion and recurrence

Identify and block the way attackers continue to access

- Identifying and blocking remote access methods
- Patch vulnerabilities
- Identification and Blocking of RAT-Infected computers

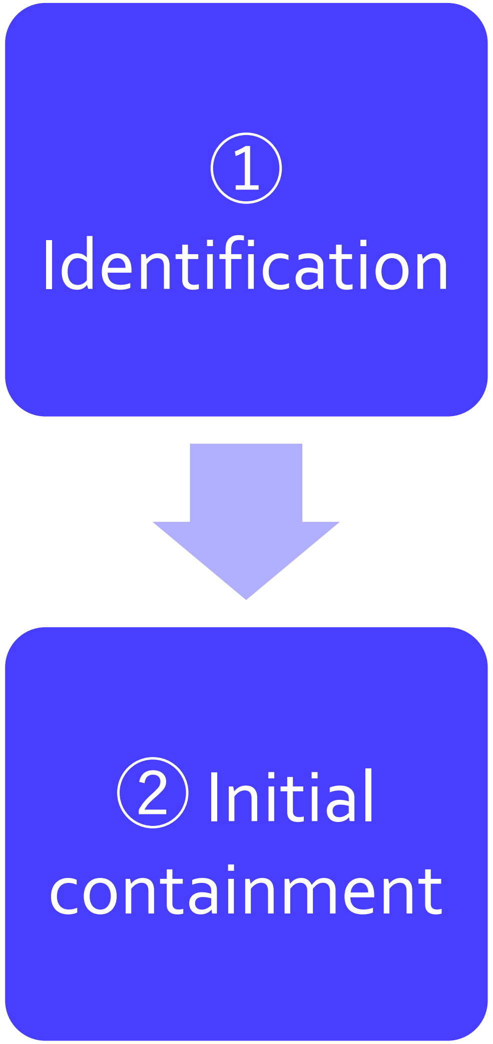
Mitigation of “Dominance” activity

- Password reset of all stolen accounts
- Limiting accessible ports of servers and computers
- Network Segmentation and access control
- Application white-list, etc

Company-wide monitoring and research

- Utilize EDR, Event logs, Client management software logs, anti-virus, etc.
- Utilize IOC findings from Investigation, create custom signatures for above security products.

Examples in a domestic incident



① Identification

- Interview
    - Two ransomware encryptions were discovered at different times
    - Logon scripts ware abused to distribute ransomware
- Investigation of AV detection log
    - SMB/RDP brute-force tools were detected by AV

② Initial containment

- Blocking all Internet connections
- Reset password for domain administrator account
- Fixed logon scripts

Examples in a domestic incident

③ Create specific response plan

Phase 1 - Implement countermeasures to ensure a certain level of safety and recover network and system within 48 hours

- Identification and countermeasures for initial intrusion routes (root cause)
- Identification of Lateral Movement techniques attacker used and implementation of mitigation measures
- Domain Controllers Safety Check
- Implement EDR and establish company-wide threat monitoring operation.

Phase 2 – Further investigation and implement additional countermeasures

- Forensics for compromised server/terminal and clarify attack details
- Update IOCs based on forensic result and continuous monitoring with EDR
- Implementation of additional countermeasures

Examples in a domestic incident

④ Investigation and Threat Hunting

Event logs	•Identifying domain Administrator Accounts were abused. •Identify the login source private IP address which attacker used to access internal computers, and identified attacker abuse VPN.
Client management software logs	•Identification of activities by the attacker (malicious file name, execution history, etc). •Extracting IOC Information •Found mstsc and PsExec are used for Lateral Movement
Domain Controller Safety Check	•Quick Triage (Persistence, Memory, FileSystem, Program Execution) •Confirmation of RAT and other malware infection in order to prevent continuous access of attacker
Establishment of a company-wide hunting system using EDR	•Urgent deployment required for devices reconnecting to the network •Use IOCs as signatures

Examples in a domestic incident

⑤ Containment

- Restricting Source IP Address that can access VPN, and Implement Certificate Authentication
- Resolving vulnerabilities in VPN devices
- Limitations of RDP/SMB access to servers and computers.
- Password reset for compromised domain administrator account
- Countermeasures for Golden Tickets attack
- Implement Detecting and preventing the execution of existing attack tools

⑥ Eradication

- Restoring a compromised terminal/server from a safe backup
- *As there was no use of RAT, the risk of continuous access is low.

Summary and Predictions for Targeted Ransomware

Domestic Ransom(ware) in 2020

Initial access – following international cases

- Vulnerable devices (On-Premise/Cloud) will continue to be compromised directly from Internet
- Ransomware downloaded by other Malware which is spreading via e-mail (Emotet, etc.) is (will be) increasing in Japan, same as overseas.
- Increasing ransomware incidents even in organizations which properly implement “Perimeter Defense”

Dominance – close to targeted attack methods

- Use of RAT and penetration testing tools such as BloodHound and other APT like tools are expected to increase in Japan.
- Use of RAT makes containment and eradication more difficult
- Attacker may repeatedly or continuously distribute ransomware using RAT in same organization, even after security team recovers their encrypted data.

Domestic Ransom(ware) in 2020

Ransom – methods other than file encryption

- **Attack on availability**
  - Attacker may find other ways to attack on availability other than encryption.
    - Changing passwords for all domain accounts
    - Interference with system operation by deleting files or changing settings on various servers
- **Attack on confidentiality**
  - Attacker may threaten organization using confidential information they steal.
    - Cases of obtaining confidential information, such as intellectual property, R & D information, and personal information, and threatening in exchange for disclosure will occur also in Japan
- **Attack on integrity**
  - Secondary damage may occur about data integrity
    - Obstruction of business by partial file wiping or encryption

Is It Wrong to Try to Find APT Techniques in Ransomware Attack?

"Targeted"?

- Attackers aren't targeting specific organizations to encrypt or steal money.
  - After widespread attacks, attacker target organizations with weak security organizations that are likely to pay ransoms or have valuable information
- Although there are the same/similar methods as targeted attacks in terms of each method, the overall attack flow is unique.

Ransom "ware"?

- Ransomware is just one way to make threats for money.
  - Attacker don't have to use "Ransomware" if there are another ways of obtaining money.
- Don’t pay too much attention to ransom”ware”. It is important in incident response to understand and prepare overall attack process.

IoC

Malware/Tool name	SHA-256 Hash
NLBrute1.2	E21569CDFAFBBDD98234EF8AFCC4A8486D2C6BA77A87A57B4730EB4A8BD63BC2
NS.exe	F47E3555461472F23AB4766E4D5B6F6FD260E335A6ABC31B860E569A720A5446
KPortScan3	080C6108C3BD0F8A43D5647DB36DC434032842339F0BA38AD1FF62F72999C4E5
SoftPerfect Network Scanner	66C488C1C9916603FC6D7EC00470D30E6F5E3597AD9F8E5CE96A8AF7566F6D89
MS16-032	9F023D74CF5E16A231660805ADFC829C1BE24A6B1FA6CB3ED41F0E37FE95062B 9AFAE820C8F7ED5616A4523A45968CFDABF646C5151A9C1DB1A6E36D7A9D1E11
rsa.exe	48303E1B50B5D2A0CC817F1EC7FA10C891F368897B0AEA2D02F22701D169CE54 E6CCB71FD62783DE625CBFCDAE1836B9FFB33B0E2344D709F5B6C5B2E6EAC8D8
mRemoteNC	3BC3038749427E1D6DA05FD3972A86F3403B40102974BD241A233EBD2C3B8C5C
mRemoteNG	9476FE1896669163248747785FA053ACA7284949945ABD37C59DAE4184760D58
Ammyy Admin	5FC600351BADE74C2791FC526BCA6BB606355CC65E5253F7F791254DB58EE7FA A0C996178FAA8320948D886F47EF394C712F1E5DC0F7C8867CD4BB1DB5F2A266
xDedicLogCleaner	878706CD11B5223C89AAEF08887B92A655A25B7C630950AFFA553574A60B922E
Advanced IP Scanner	02EC949206023F22FE1A5B67B3864D6A653CC4C5BFCB32241ECF802F213805E8
PCHunter	D1AA0CEB01CCA76A88F9EE0C5817D24E7A15AD40768430373AE3009A619E2691

Secureworks®