

# ランサムウェアに標的型攻撃手法を 求めるのは間違っているだろうか

セキュアワークス株式会社

玉田 清貴

山崎 景太

中津留 勇

2020/01/17

Japan Security Analyst Conference 2020

Secureworks®

# Agenda

- 標的型ランサムウェアインシデントの概要
- 標的型ランサムウェアインシデント事例
- 標的型ランサムウェアインシデントの調査結果
  - Tactics, Techniques, and Procedures
    - 侵入
    - 掌握(権限昇格、情報収集、横展開)
    - 脅迫
    - 痕跡消去
  - 標的型攻撃との比較
- 推奨する対策
  - 予防、インシデントレスポンス、事後対応など
- まとめと今後の脅威の展望予測





# 標的型ランサムウェアインシデントの概要

# ランサムウェアを利用した攻撃手法の変化



CryptoLocker(2013/09)



Wannacry (2017/05)

~2017

メール添付やドライブ  
バイダウンロードにより感  
染

2017

Wannacry による大規  
模インシデント

MS17-010 の脆弱性の  
ある公開サーバ経由で  
組織内ネットワーク内に  
感染拡大

2018~

ネットワーク内での  
様々な侵害行為を  
伴うケースが発生  
組織の規模やリピー  
ト数に応じて復号価  
格が変動

biifaiclosta1985@protonmail.com

## Ryuk

balance of shadow universe

# 標的型ランサムウェアインシデントの典型

## 侵入

- 広範囲に攻撃を行い、侵入できる組織を探す

## 掌握

- 権限昇格, 情報収集, 横展開を行い、可能な限り組織のネットワークを掌握する

## 脅迫

- ランサムウェアを用いて大規模な暗号化を実施

## 痕跡削除

- ランサムウェアの機能やコマンド・ツールを用いて痕跡を消去する



# 標的型ランサムウェアインシデント事例

本セッションは  
会場のみでの公開になります





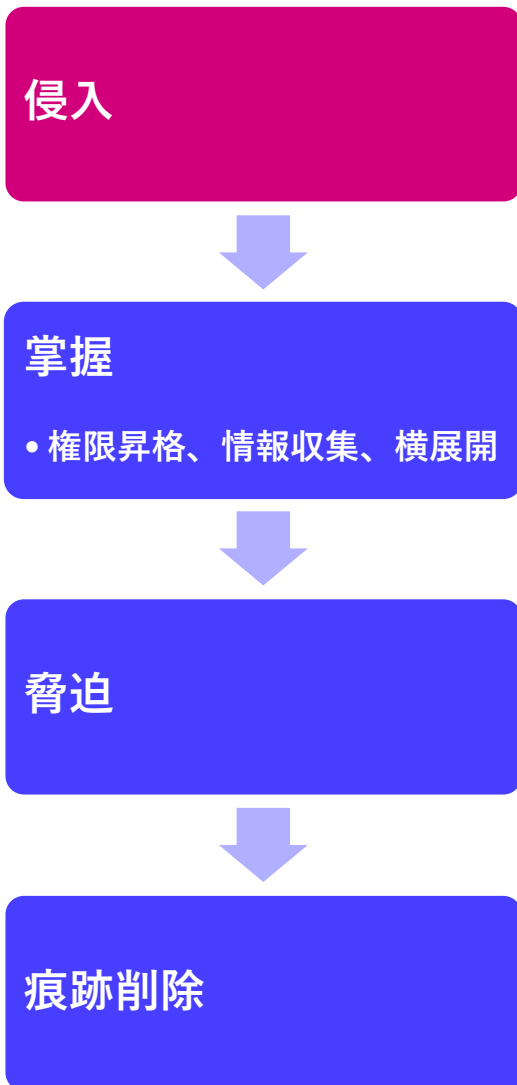
# 標的型ランサムウェアインシデントの 調査結果



# Tactics, Techniques, and Procedures

## 標的型ランサムウェアインシデントの調査結果

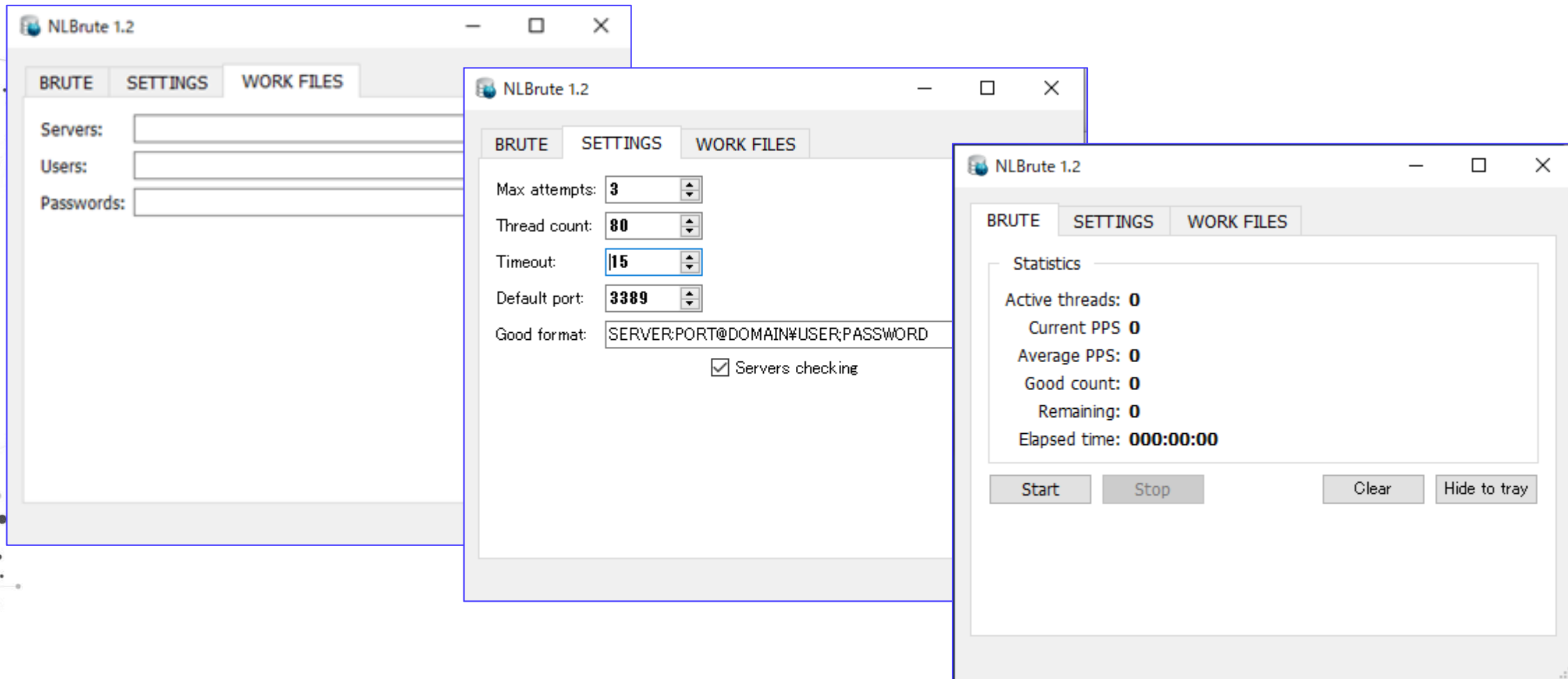
# 侵入の手法



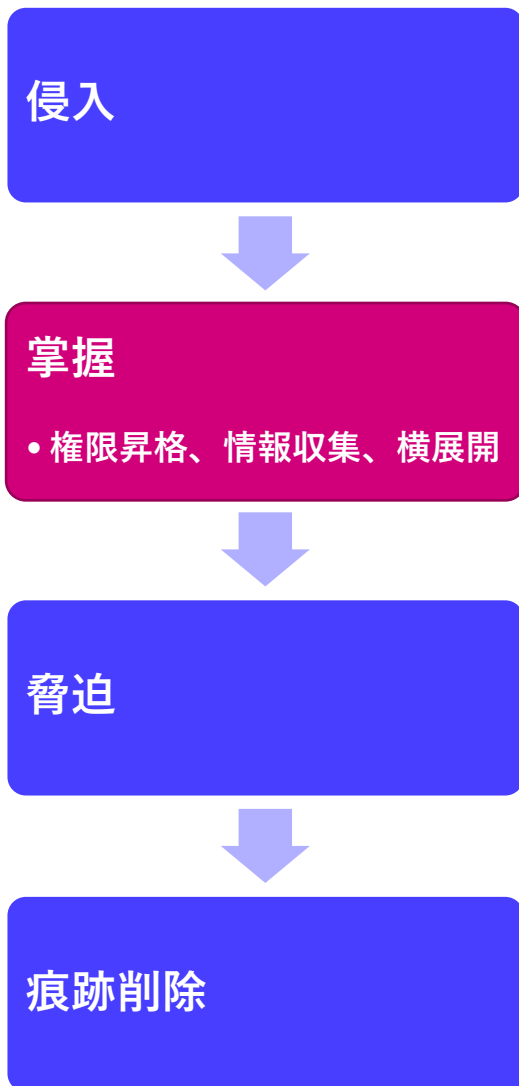
- 国内・海外事例で確認
  - 公開されているRDPやVPN経由
    - NLBruteなどのブルートフォースツールを利用して脆弱なパスワードを突破
  - メールに添付されたマルウェア経由
    - Emotet経由(その後TrickBotをダウンロード)
- 国内事例のみで確認
  - グローバルIPが割り当てられたモバイルデータ通信端末 + MS17-010 の脆弱性
- 海外事例のみで確認
  - Dridex(Bugat v5)経由
  - CobaltStrike経由
  - Empire経由
  - Meterpreter経由

# NLBrute

IPリスト、ユーザ名リスト、パスワードリストを用意してブルートフォースを実施するツール



# 権限昇格の手法



- 国内・海外事例で確認
  - Mimikatzを利用したパスワードダンプ
    - TrickBotやEmpireなどのモジュールを利用
  - 侵入時のアカウントが管理者権限であることが多い
- 国内事例のみで確認
  - Githubに公開されている特定の脆弱性のPoCツールを利用

# 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: 00000000
Couldn't open process token 5

c:\Users\John\Desktop\work>
```

管理员: C:\Windows\system32\cmd.exe

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

```
C:\Windows\system32>whoami
nt authority\system
```

```
C:\Windows\system32>
```

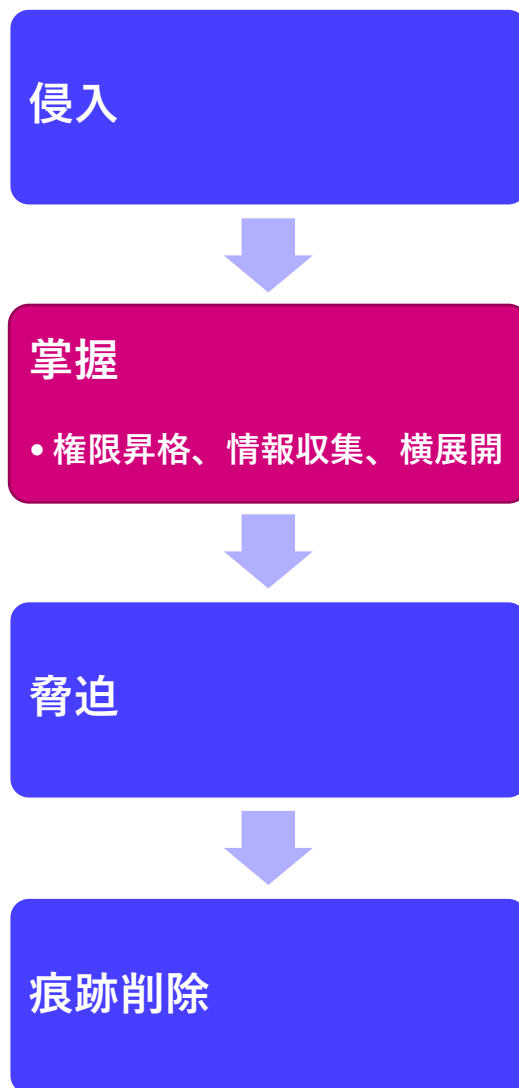
- MS13-005
- MS13-046
- MS13-053
- MS14-002
- MS14-040
- MS14-058
- MS14-066
- MS14-068
- MS14-070
- MS15-001
- MS15-010
- MS15-015
- MS15-051
- MS15-061

- 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

# TrickBotのMimikatzモジュール

名前	更新日時	種類	サイズ
injectDll32_configs	2019/12/16 17:00	ファイル フォルダー	
networkDll32_configs	2019/12/16 17:00	ファイル フォルダー	
psfin32_configs	2019/12/16 17:00	ファイル フォルダー	
pwgrab32_configs	2019/12/16 17:00	ファイル フォルダー	
importDll32	2019/10/17 4:28	ファイル	7,430 KB
injectDll32	2019/10/19 5:03	ファイル	364 KB
networkDll32	2019/10/16 5:24	ファイル	19 KB
psfin32	2019/10/19 5:03	ファイル	19 KB
pwgrab32	2019/10/19 5:03	ファイル	1,093 KB
systeminfo32	2019/10/19 5:03	ファイル	17 KB
tabDll32	2019/10/19 5:03	ファイル	625 KB

# 情報収集の手法



- 国内・海外事例で確認
  - マルウェアの機能を用いたスキャンおよび情報収集を実施
- 国内事例のみで確認
  - Advanced IP ScannerやAdvanced Port Scanner、SoftPerfect Network Scanner、ProcessHacker、KPortScan3、PowerToolsなどを利用
- 海外事例のみで確認
  - Hyenaを利用
  - BloodHoundやSharpHoundを利用したAD探索

# Advanced IP Scanner

<https://www.advanced-ip-scanner.com/jp/>

Advanced IP Scanner

ファイル(F) 操作(A) 設定(S) ビュー(V) ヘルプ(H)

スキャン

10.0.0.1 - 10.255.255.254

結果 お気に入り

状態	名前	IP	製造社	MACアドレス	コメント
	7.0.0.10.in-addr.arpa	10.0.0.7	VMware, Inc.	00:0C:29:04:10:89	
	John-PC	10.0.0.10	VMware, Inc.	00:0C:29:5A:7F:25	
	101.0.0.10.in-addr.arpa	10.0.0.101	VMware, Inc.	00:0C:29:A7:7E:26	
	HTTP, Apache				It works (Apache httpd 2.4.7)
	cases				
	mnt				
	share				
	110.0.0.10.in-addr.arpa			00:0C:29:39:77:7C	
	HTTP, INetSi				
	FTP (ftp)				
	253.0.0.10.in-addr.arpa			00:50:56:C0:00:01	
	254.0.0.10.in-addr.arpa			00:0C:29:FB:AA:35	

検索

Radmin

ツール

コピー

保存...

お気に入りに追加

名前の変更

コメントを編集

詳細

フルコントロール

表示のみ

Telnet

ファイル転送

シャットダウン

チャット

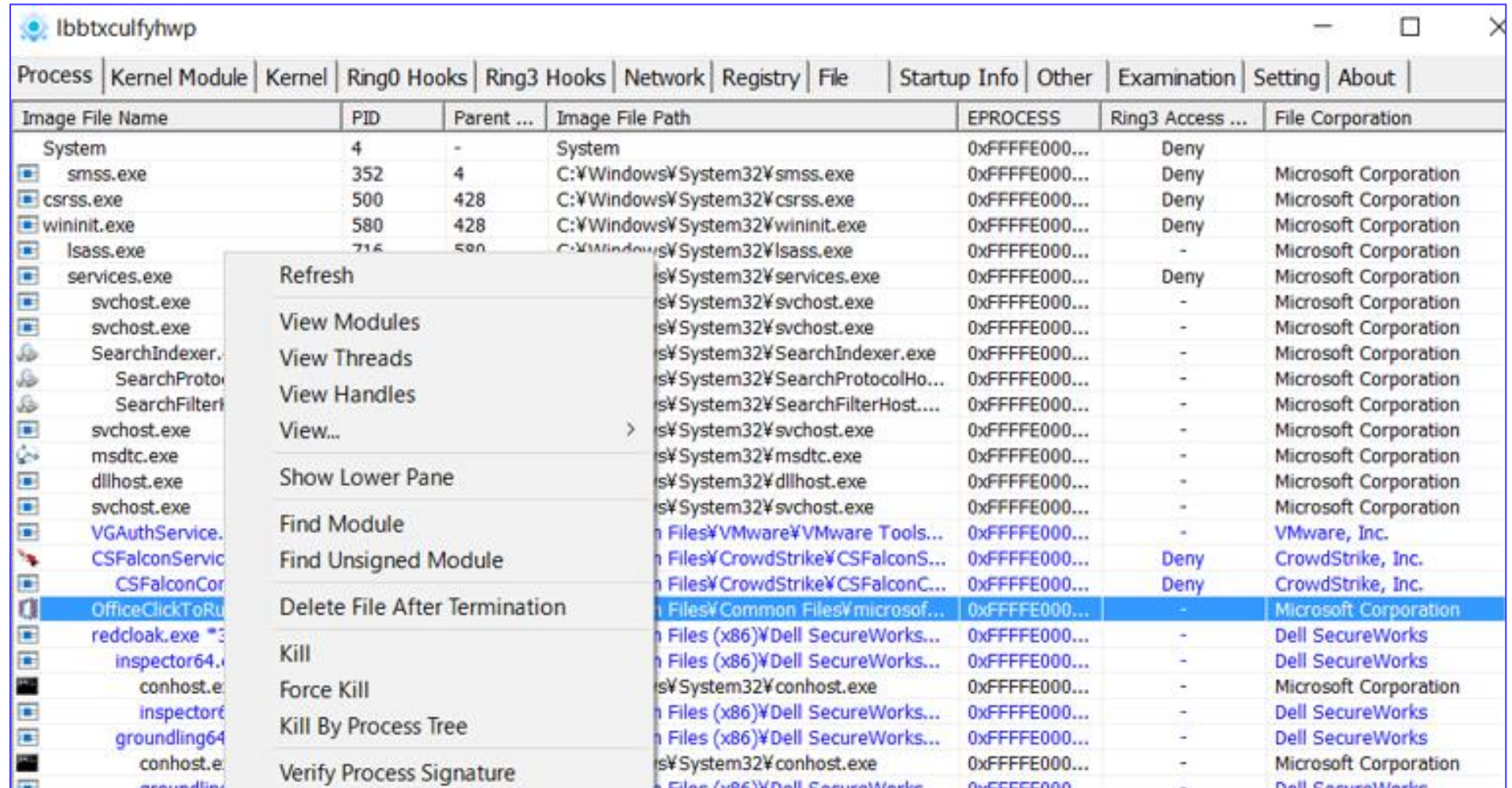
音声チャット

メッセージの送信



# PCHunter

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



The screenshot shows the PC Hunter application window titled 'lbbtxculfyhwp'. The interface includes a menu bar with options: Process, Kernel Module, Kernel, Ring0 Hooks, Ring3 Hooks, Network, Registry, File, Startup Info, Other, Examination, Setting, and About. Below the menu bar is a table listing system processes. A context menu is open over the 'OfficeClickToRun' process, showing various actions such as Refresh, View Modules, View Threads, View Handles, View..., Show Lower Pane, Find Module, Find Unsigned Module, Delete File After Termination, Kill, Force Kill, Kill By Process Tree, and Verify Process Signature.

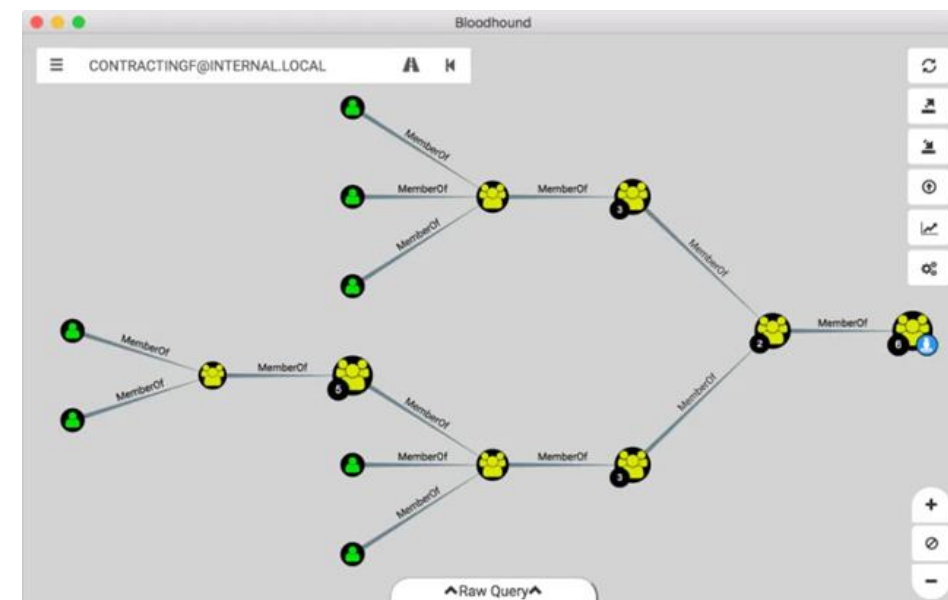
Image File Name	PID	Parent ...	Image File Path	EPROCESS	Ring3 Access ...	File Corporation
System	4	-	System	0xFFFFE000...	Deny	
smss.exe	352	4	C:\Windows\System32\smss.exe	0xFFFFE000...	Deny	Microsoft Corporation
csrss.exe	500	428	C:\Windows\System32\csrss.exe	0xFFFFE000...	Deny	Microsoft Corporation
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			C:\Windows\System32\services.exe	0xFFFFE000...	Deny	Microsoft Corporation
svchost.exe			C:\Windows\System32\svchost.exe	0xFFFFE000...	-	Microsoft Corporation
svchost.exe			C:\Windows\System32\svchost.exe	0xFFFFE000...	-	Microsoft Corporation
SearchIndexer.exe			C:\Windows\System32\SearchIndexer.exe	0xFFFFE000...	-	Microsoft Corporation
SearchProtocolHost.exe			C:\Windows\System32\SearchProtocolHost.exe	0xFFFFE000...	-	Microsoft Corporation
SearchFilterHost.exe			C:\Windows\System32\SearchFilterHost.exe	0xFFFFE000...	-	Microsoft Corporation
svchost.exe			C:\Windows\System32\svchost.exe	0xFFFFE000...	-	Microsoft Corporation
msdtc.exe			C:\Windows\System32\msdtc.exe	0xFFFFE000...	-	Microsoft Corporation
dllhost.exe			C:\Windows\System32\dllhost.exe	0xFFFFE000...	-	Microsoft Corporation
svchost.exe			C:\Windows\System32\svchost.exe	0xFFFFE000...	-	Microsoft Corporation
VGAAuthService.exe			C:\Program Files\VMware\VMware Tools\bin\... \VGAAuthService.exe	0xFFFFE000...	-	VMware, Inc.
CSFalconService.exe			C:\Program Files\CrowdStrike\CSFalconService.exe	0xFFFFE000...	Deny	CrowdStrike, Inc.
CSFalconControlPanel.exe			C:\Program Files\CrowdStrike\CSFalconControlPanel.exe	0xFFFFE000...	Deny	CrowdStrike, Inc.
OfficeClickToRun.exe			C:\Program Files\Microsoft Office\Office16\OfficeClickToRun.exe	0xFFFFE000...	-	Microsoft Corporation
redcloak.exe			C:\Program Files (x86)\Dell SecureWorks\redcloak.exe	0xFFFFE000...	-	Dell SecureWorks
inspector64.exe			C:\Program Files (x86)\Dell SecureWorks\inspector64.exe	0xFFFFE000...	-	Dell SecureWorks
conhost.exe			C:\Windows\System32\conhost.exe	0xFFFFE000...	-	Microsoft Corporation
inspector64.exe			C:\Program Files (x86)\Dell SecureWorks\inspector64.exe	0xFFFFE000...	-	Dell SecureWorks
groundling64.exe			C:\Program Files (x86)\Dell SecureWorks\groundling64.exe	0xFFFFE000...	-	Dell SecureWorks
conhost.exe			C:\Windows\System32\conhost.exe	0xFFFFE000...	-	Microsoft Corporation
groundling64.exe			C:\Program Files (x86)\Dell SecureWorks\groundling64.exe	0xFFFFE000...	-	Dell SecureWorks

# BloodHound/SharpHound

<https://github.com/BloodHoundAD/BloodHound>



- Active Directory 環境における隠れた関係と攻撃パスを明らかにするツール
  - NW上のPC/サーバにおけるユーザ名、コンピュータ名、グループ、ドメイン、OUなどの情報を集約し関連性を可視化し、ADサーバへの攻撃経路を特定することが可能
- SharpHound は BloodHound Ingestor のC#バージョン
  - 高速・安定に動作する



引用: <https://waldo.com/?p=68>

# NS.exe (NetworkShare)

## NW共有フォルダ探索ツール

```
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 address for scan network:
```

```
1 Scan by: 192.168.0.0
```

```
2 Scan by:
```

```
3 Scan by:
```

```
13 Scan all
```

```
Enter a number
```

```
Get ip: 192.168.1.1
```

```
start scan for
```

```
host 192.168.1.1
```

```
do  
{  
    shared_path = malloc(0x208u);  
    v24 = shared_path;  
    memset(shared_path, 0, 0x208u);  
    wprintfW(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_Users )  
    {  
        wprintf(L"-Found share \\\\\\%s\\%s\\n", &servername, netshare->shi502_netname);  
        addconnection_result = aa_WNetAddConnection2W(shared_path);  
        if ( addconnection_result == ERROR_ALREADY_ASSIGNED )  
        {  
            continue;  
        }  
    }  
}
```

# 横展開の手法

侵入



掌握  
• 権限昇格、情報収集、横展開



脅迫



痕跡削除

- 国内・海外事例で確認
  - RDPやPsExec、WMI経由で実施
- 国内事例のみで確認
  - MRemoteNG、MRemoteNCやPutty、Ammy Adminなどを利用
  - bruttolineを利用したブルートフォースによるパスワード突破の実施
- 海外事例のみで確認
  - EmpireやCobaltStrike、reGeorgを利用

# mRemoteNG

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

The image displays two screenshots of the mRemoteNG application interface. The left screenshot shows the main configuration window with a table of hosts and a 'Display' panel. The right screenshot shows the 'External Tools' menu and the 'External Tool Properties' dialog.

**Table of Hosts (Left Screenshot):**

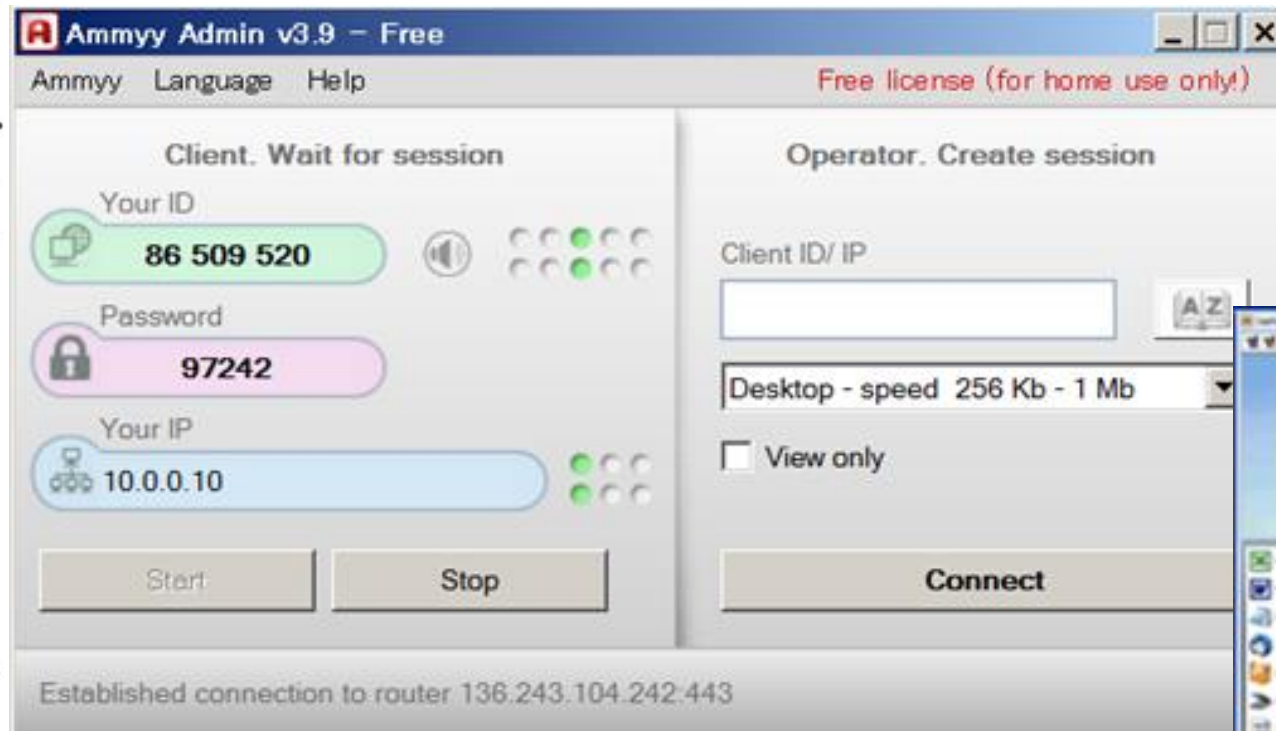
Hostname/IP	SSH	Telnet	HTTP	HTT...	Rlogin	RDP	VNC	Open Ports
10.0.0.252	No	No	No	No	No	No	No	
10.0.0.251	No	No	No	No	No	No	No	
10.0.0.250	No	No	No	No	No	No	No	
10.0.0.249	No	No	No	No	No	No	No	
10.0.0.248	No	No	No	No	No	No	No	
10.0.0.247	No	No	No	No	No	No	No	
10.0.0.246	No	No	No	No	No	No	No	
10.0.0.243	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	

**External Tool Properties (Right Screenshot):**

- Display Name: [Empty]
- Filename: [Empty]
- Arguments: [Empty]
- Working directory: [Empty]
- Options:  Wait for exit,  Run elevated,  Try to integra,  Show On Too

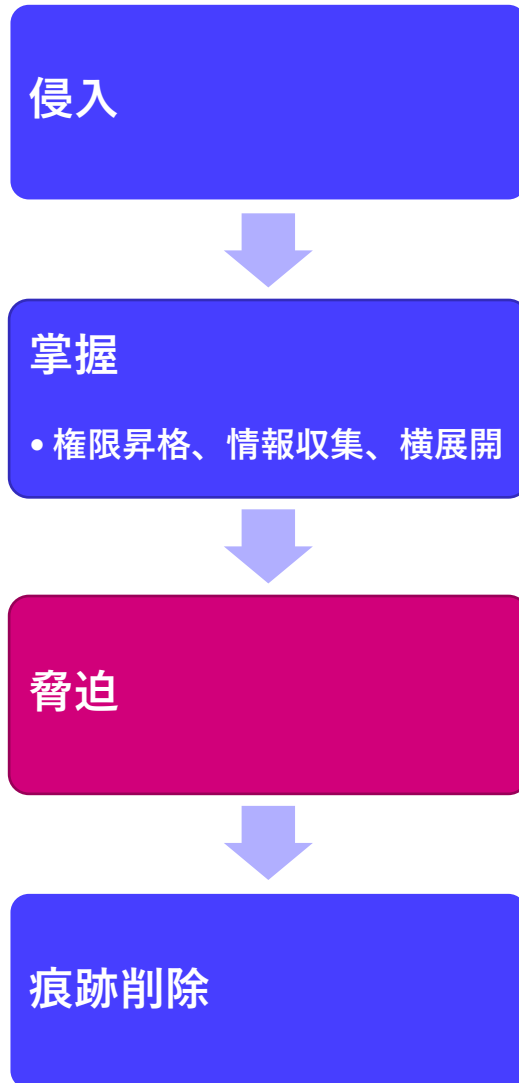
# Ammy Admin

<http://www.ammy.com/en/>



引用: [http://www.ammy.com/en/admin\\_screenshots.html](http://www.ammy.com/en/admin_screenshots.html)

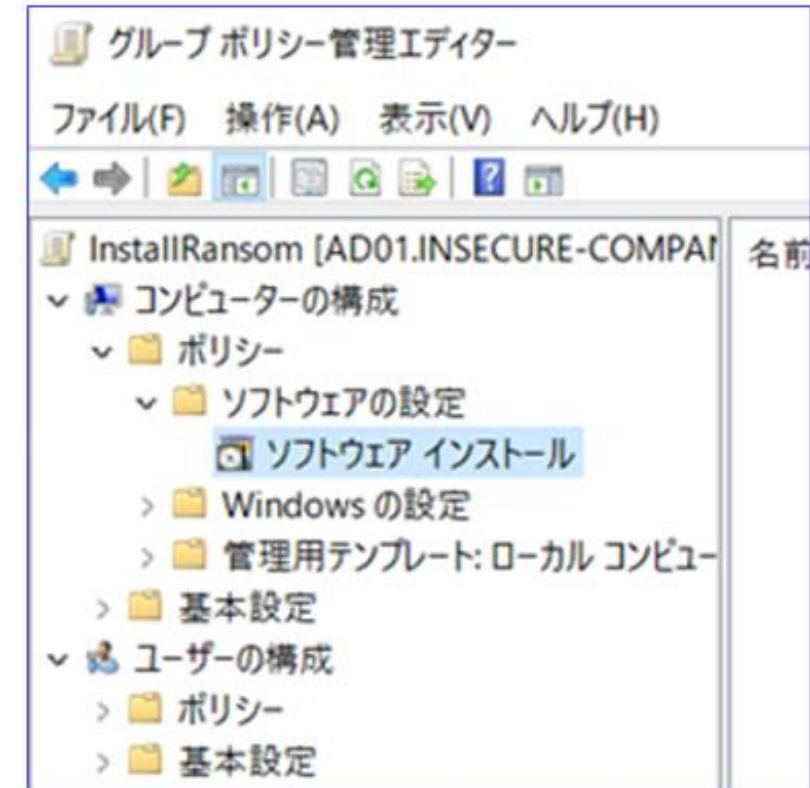
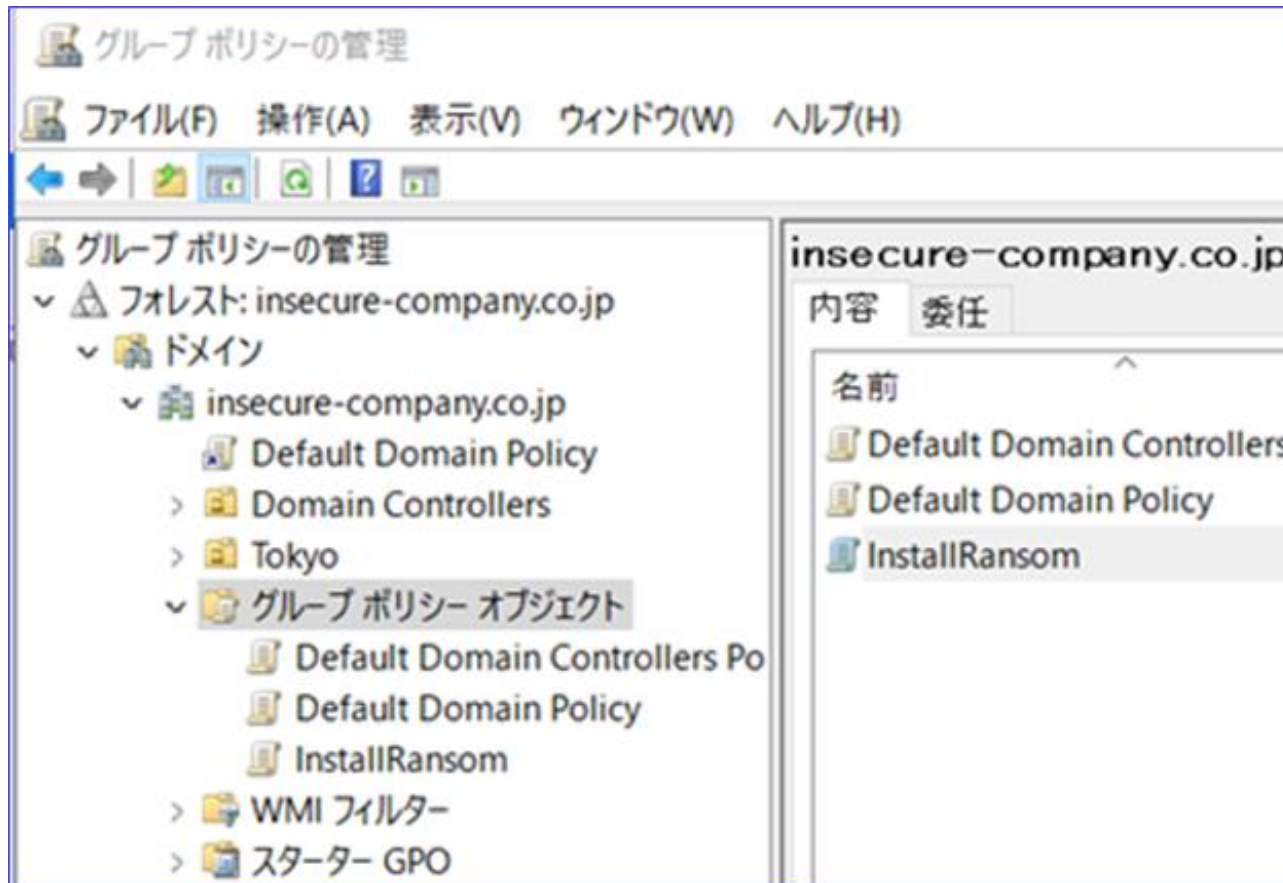
# 脅迫の手法



- 国内・海外事例で確認
  - PsExecやRDP、WMIを利用して1台ずつランサムウェアを実行
  - RATやpost-exploitation frameworkの機能によりランサムウェアを展開・実行
  - バッチファイルやPowershellスクリプトを利用
  - ADサーバ経由でグループポリシーやログオンスクリプトを用いてドメイン配下の端末にランサムウェアを一斉配信
  - ランサムウェアの種類は様々

# ADサーバからのランサムウェア配信

グループポリシーを使用してランサムウェアを一斉配信する





# ADサーバからのランサムウェア配信

## ログオンスクリプトを利用したランサムウェアの自動実行

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 -

# 利用されるランサムウェアの種類

Matrix

Phobos

GandCrab

GlobelImposter

Clop

Dharma

Ryuk

MedusaLocker

Frendi

CrySiS

Scarab

Samsam

BitPaymer

Defray777

REvil  
/ Sodinokibi

rsa.exe /  
aes.exe

# ランサムウェアの代表的な機能

## ファイル暗号化

- RSA-2048, RSA-4096とAES-256の組み合わせ
- ファイル中のデータを高速なAESで暗号化して、利用したAES秘密鍵をRSA公開鍵で暗号化する

## 暗号化範囲拡大

- A-Zドライブの探索
- NW共有フォルダ、管理共有などの探索
- FW無効化

## 復号、フォレンジック対策

- VSS消去
- スタートアップ修復の無効化

## 脅迫文の表示

# コマンドラインツール **rsa.exe**

ランサムウェアだが暗号化ツールに近い

```
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>
```

# コマンドラインツール **rsa.exe**

## Usage の無いバージョンなど複数存在

```
5  if ( argc == 2 )
6  {
7      sub_4028E0();
8      if ( lstrcmpiA(argv[1], k) )
9      {
10         if ( lstrcmpiA(argv[1], rk) )
11         {
12             if ( lstrcmpiA(argv[1], e) )
13             {
14                 if ( lstrcmpiA(argv[1], d) )
15                     Usage(*argv);
16                 else
17                     DecryptFile();
18                 result = 0;
19             }
20         }
21         else
22         {
23             EncryptFile();
24             result = 0;
25         }
26     }
27 }
```

Usage があるバージョン

Usage が無いバージョン  
(引数をつけなければ暗号化を行う)

```
7  if ( argc == 1 )
8      goto LABEL_2;
9  if ( argc == 2 )
10 {
11     if ( lstrcmpiA(argv[1], k) )
12     {
13         if ( lstrcmpiA(argv[1], rk) )
14         {
15             if ( !lstrcmpiA(argv[1], e) )
16             {
17 LABEL_2:
18                 EncryptFile();
19                 return 0;
20             }
21             if ( lstrcmpiA(argv[1], d) )
22                 nullsub_4(*argv);
23             else
24                 DecryptFile();
25             result = 0;
26         }
27     }
```



# 感染範囲拡大、復号対策時に利用される コマンド例

- 感染範囲拡大
  - "netsh advfirewall set currentprofile state off"
  - "netsh firewall set opmode mode=disable"
- 復号対策
  - "wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0"
  - "vssadmin delete shadows /all /quiet"
  - "wmic shadowcopy delete /nointeractive"
  - "bcdedit /set {default} bootstatuspolicy ignoreallfailures"
  - "bcdedit /set {default} recoveryenabled no"
- 証拠隠蔽
  - "C:¥Windows¥system32¥cmd.exe" /c del <マルウェア実行パス>¥<マルウェア名> > nul

# ランサムウェアにハードコードされたコマンド

## 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);
```

# 脅迫文

ビットコインの振り込みではなく、直接コンタクトを要求する形が主流



## 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 u

Otherwise, you never cant return your data.

For purchasing a decryptor contact us by email:

[Erenahen@cock.li](mailto:Erenahen@cock.li)

If you will get no answer within 24 hours contact us by our alternate emails:

[Kishemez@tutanota.com](mailto: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 f

## 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:

[Folieboi@protonmail.com](mailto:Folieboi@protonmail.com)

If you will get no answer within 24 hours contact us by our alternate emails:

[Ctorsenoria@tutanota.com](mailto: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 (no more than 10Mb). Indicate your personal ID on the letter:

EDA13DD7A7FA0E99841FFB96A9BBDAA...CAF98700233124C9C3BD886D4974331D5797D7187C64...

800141DC6E703FCE7371315A...3E139580B70F5C

1470FC81C2D89ED48F7A5161...03F54650B1C710F

B075006C3E1DEC731A31A969...EBBB19D10A42AD

ECA1B2EC049A382F20D8692F...888E35823E29A3

7664545763FA2AECED29932F1...18C2B6E37DCF5E

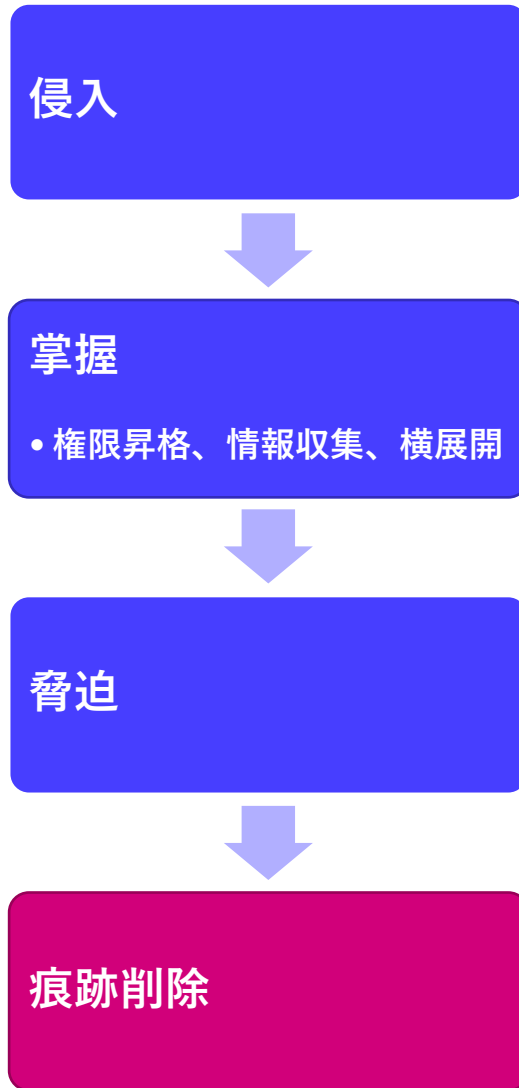
188AD731FE50504A646889E8F...EFD4819DE3A114

D855FE6D40CF9761CAD93775...ECBC0F259D9DE4


ランサムウェアが作成する脅迫文だけでなく、メモ帳で手入力しているケースも



# 痕跡消去の手法



- 国内・海外事例で確認
  - ランサムウェアの機能でVSS消去、FW無効化
  - sdelete.exe -p 5 <FileName>でファイル削除
  - pslog.exe -c securityなどの実施
  - 国内・国外ともに痕跡消去を行っていないケースも多数ある
  - ランサムウェアの動作により一部レジストリ/イベントログ/その他ファイルの暗号化によって副次的に痕跡が消去される
- 国内事例のみで確認
  - xDedicLogCleanerの利用

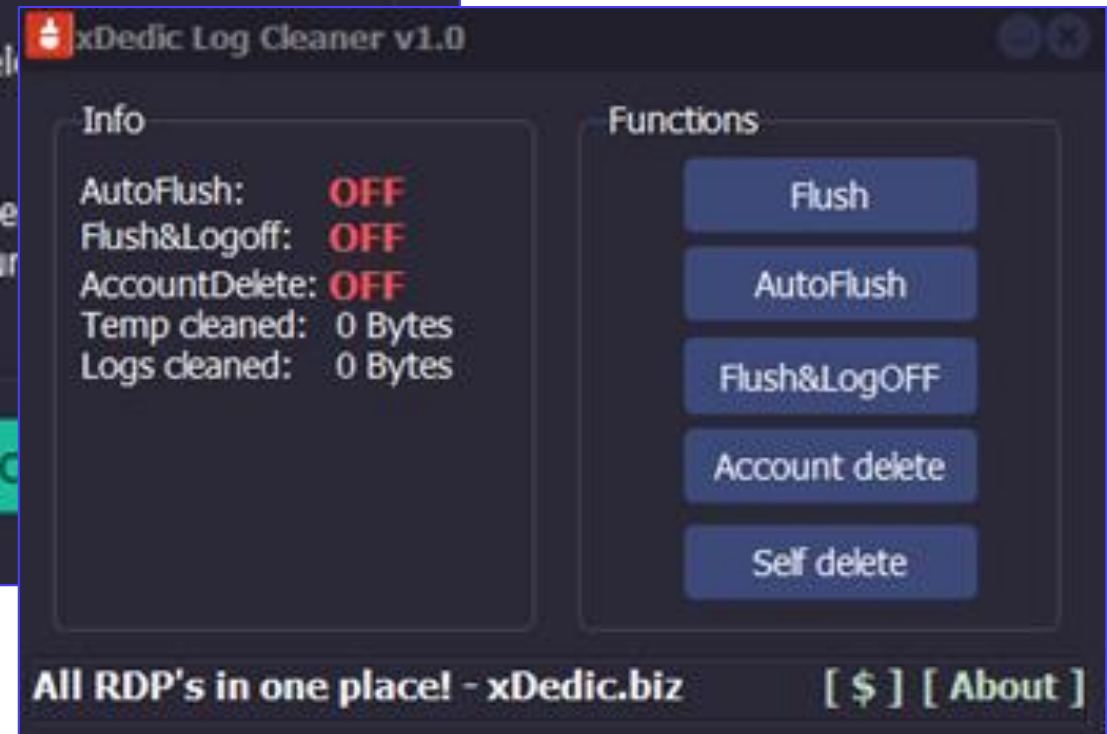
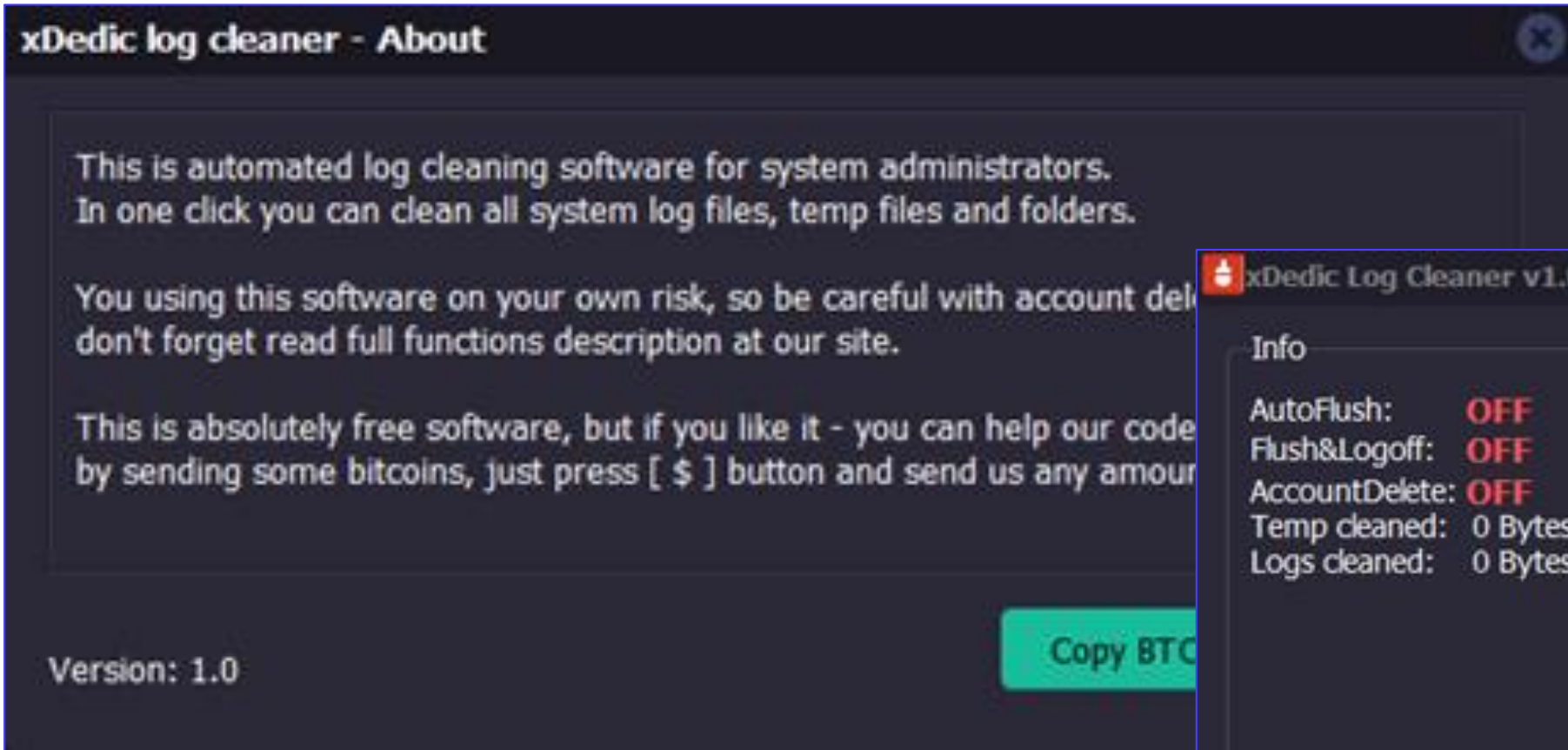


# PowerShellを用いたセキュリティ製品のアンインストール

- 実行履歴
  - C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥PowerShell¥PSReadline¥ConsoleHost\_history.txt
- コマンド
  - (Get-WmiObject -Class Win32\_Product -Filter "Name='Symantec Endpoint Protection'" -ComputerName .).Uninstall()
  - (Get-WmiObject -Class Win32\_Product -Filter "Name='Endpoint Protection'" -ComputerName .).Uninstall()

# xDedicLogCleaner

ワンクリックでPC内の様々な履歴を消去





# 標的型攻撃との比較

## 標的型ランサムウェアインシデントの調査結果

# 各事例における攻撃の流れ

## 事例によって大きく異なる TTPs

	侵入	掌握	脅迫	痕跡削除
国内・海外 <sub>1</sub>	メール (Emotet)	TrickBot	Ryuk	N/A
国内 <sub>2</sub>	RDP	MS16-032, NLBrute, Advanced IP Scanner, AmmyAdmin, NetworkShare.exe	Matrix	N/A
国内 <sub>3</sub>	RDP	Advanced Port Scanner, ProcessHacker NetworkShare.exe	Phobos	N/A
国内 <sub>4</sub>	RDP	PCHunter, ProcessHacker, Mimikatz	Phobos	N/A
国内 <sub>5</sub>	RDP	KPortScan3, SoftPerfectNetworkScanner, Powertools, mRemoteNG, BruttoLine, Putty, ProcessHacker, Mimikatz	GandCrab	xDedicLogCleaner
国内 <sub>6</sub>	VPN	PsExec DomainUser 一覧表示バッチファイル	rsa.exe	pslog.exe sdelete.exe
国内 <sub>7</sub>	RDP	PsExec	GlobeImposter2.0	N/A
海外 <sub>2</sub>	RDP	Hyena, Mimikatz, WMIexec, reGeorg	Samsam	N/A
海外 <sub>3</sub>	メール (Dridex)	Empire, PsExec	BitPaymer	N/A
海外 <sub>4</sub>	メール	CobaltStrike, Meterpreter, SharpHound	Defray777	N/A

# 標的型攻撃に対する標的型ランサムウェアの特徴

- 様々な組織に侵入を試み、セキュリティ対策が甘く、ランサムウェアの展開が容易な標的に対して攻撃を行う
- パスワード突破の際にブルートフォースを多用する
- フリーツールを多用して標的システムの掌握を行う
- ADサーバのソフトウェアインストールやログオンスクリプトなどのグループポリシーの機能を活用する
- 利用するランサムウェアが多用で、種類やバージョンの入れ替わりが速い
- 海外事例は標的型攻撃 (ペネトレーションテスト) の TTPs に近い事例が多い



# 推奨する対策

# インシデント発生前の準備

以下の観点で、対策・計画を準備する



1. 攻撃の妨害



2. 検知と初期封じ込め



3. 被害発生後の対応



# 1. 攻撃の妨害

- 「侵入」、「掌握」、「脅迫」を防止するための対策を実装し、攻撃成功までのコストを上げる
  - 標的型攻撃と異なり、攻撃が容易な組織で被害が発生・拡大する

## 「侵入」の対策

- FW(ネットワーク, パーソナル, セキュリティグループ for クラウド等)
- VPN及びその他ネットワーク機器の脆弱性管理
- メールセキュリティ
- アンチウイルス

## 「掌握」の対策

- ネットワークセグメンテーションとアクセス制御
- アプリケーションホワイトリスト等
- 管理アカウント管理の徹底
- ドメインコントローラの保護

## 「脅迫」の対策

- 適切なデータアクセス制限
- 安全なバックアップの取得・保管
- ファイル暗号化の検知・防御が可能なエンドポイントセキュリティの導入

## 2. 検知と初期封じ込め

- 既存のセキュリティ製品でも、何らかのインシデント発生の兆候が検知可能
  - 標的型攻撃と異なり、攻撃のステルス性は低い
- 暗号化させないための迅速な初期封じ込めが必要
  - 初期封じ込めの計画策定が重要

### セキュリティアラートの監視

- アンチウイルス
- EDR
- メール
- 管理アカウントの使用
- VPN

### アラートから脅威種別を識別する

- 発見されたマルウェア・攻撃ツール種別
- 高い権限のアカウントの利用
- 「掌握」に関わる活動

### 迅速な初期封じ込め計画の策定

- 侵害端末の隔離
- 社内ネットワークの予防的な遮断
- インターネット接続の予防的な遮断
- 管理アカウントのパスワードリセット

# 3. 被害発生後の対応

- 取得・保管したバックアップから事業影響を踏まえて迅速に復旧を実施するために計画が必要
  - ただバックアップを取得しておくだけでは不十分
- 標的型攻撃と同様に、調査・封じ込め・根絶の各プロセスについても計画を事前に策定しておく必要がある

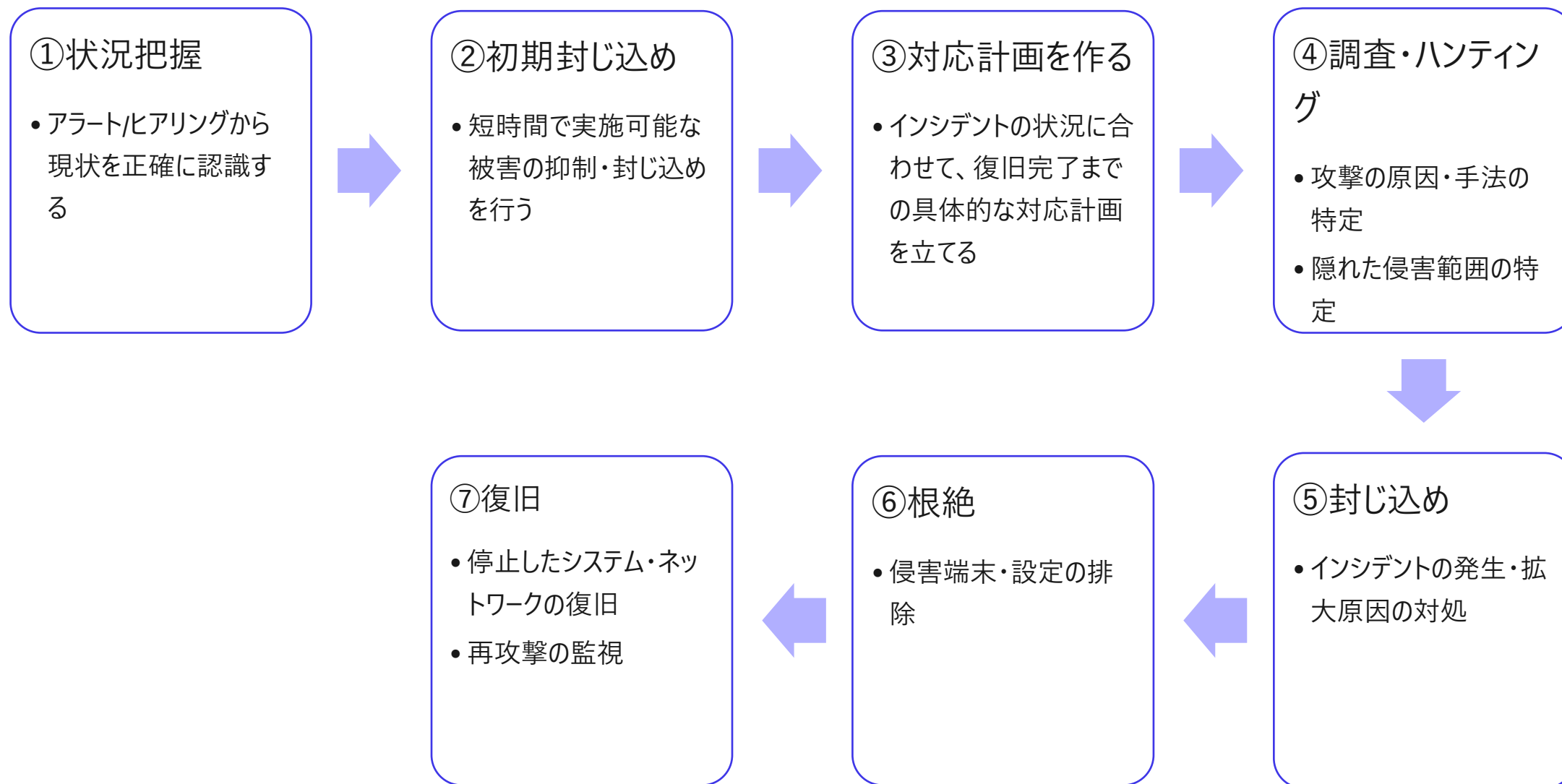
## 暗号化被害の復旧計画の策定

- システム復旧の優先順位
- 目標復旧時間の明確化
- コールドスタンバイなシステムの用意
- 復旧を行うための人員・手順書

## 「調査」、「封じ込め」、「根絶」計画の策定

- 人員・体制・コスト
- 許容される対応時間
- 各ステージで達成すべき対応の目標
- 具体的なタスク・手順の整備

# インシデント対応のプロセスとポイント



# 事業継続と安全性のバランス

- 業務停止に直結するため、システムの復旧が優先される場合がほとんど
- 先のインシデント対応プロセスをStep By Stepで実施できないケースも
- 限られた時間の中で、事業継続と安全性のバランスを取った対応プランを立案する必要がある
- 攻撃の再発や被害の拡大を防ぐために、最低限抑えるべきポイントは何か？

国内・海外のインシデント事例/対応事例を、  
広くインシデントハンドラーに共有し、  
ベストプラクティスを醸成することが特に重要

# 被害拡大・再発防止のための重要ポイント

## 攻撃者の継続的なアクセス方法を特定し遮断する

- リモートアクセス経路の特定・遮断
- 脆弱性の解消
- RAT感染端末の特定と遮断

## 掌握活動の妨害・緩和

- 窃取されたアカウントのリセット
- 各サーバ・端末のアクセス可能なポート・サービスの制限

## 全社的な監視と調査

- EDR、イベントログ、クライアント管理ソフトウェア、アンチウイルス等の活用
- 調査により判明したIOCを反映

# 具体的な対応の事例

## ①状況 把握

- ヒアリング
  - 異なる日時に、2回ランサムウェアによる暗号化が発生したことが判明
  - 後に発生した暗号化ではログオンスクリプトが悪用されていることが判明
- AV検知ログの調査
  - SMB/RDPのブルートフォースツールの検知

## ②初期 封じ込め

- インターネット接続の遮断
- ドメイン管理者アカウントのパスワードリセット
- ログオンスクリプトの修正



# 具体的な対応の事例

## ③対応計画を作る

Phase 1 - 一定の安全性を担保するための対策を行い、48時間以内にネットワーク復旧・業務を再開する

- 侵入経路(根本原因)の特定と対策
- Lateral Movement手法の特定と緩和策の実装
- ドメインコントローラの安全性の確認
- EDRによる全社監視体制の構築

Phase 2 - インシデントの全容解明とより強固な再発防止を行う

- 侵害されたサーバ・端末の詳細フォレンジック
- IoCの更新とEDRによる継続監視
- 不足している対策の実装



# 具体的な対応の事例

## ④ 調査・分析

### イベントログの分析

- 不正利用された管理者アカウントの特定
- ログイン元IPアドレス(VPN)の特定

### クライアント管理ソフトウェアの利用

- 攻撃者による活動(不正ファイル名、実行履歴、etc)の特定
- IOC情報の抽出
- mstsc及びPsExec悪用の確認

### ドメインコントローラの安全確認

- クイックリターン(Persistence, Memory, FileSystem, Program Execution)
- RAT及び継続的に侵入されるバックドア有無の確認

### EDRによる全社ハンティング体制の構築

- ネットワークに再接続する端末については緊急導入を必須に
- 発見したIOCをシグネチャとして利用

# 具体的な対応の事例

## ⑤ 封じ込め

- VPN接続元IPアドレスの制限・証明書認証の必須化
- ネットワーク機器の脆弱性解消
- RDP/SMB接続可能な端末・サーバの制限
- 侵害されたドメインアカウント/ドメイン管理者アカウントのパスワードリセット
- Golden Ticketの無効化
- 既存の攻撃ツールの検知・実行防止

## ⑥ 根絶

- 侵害された端末/サーバのセーフバックアップからの復元
- ※RATの利用等がなかったため、継続的なアクセスの危険性は低



# まとめと今後の脅威の展望予測

# 2020年及び今後の国内ランサム(ウェア)

## 侵入 – 海外事例に追従

- インターネットから直接脆弱なデバイス(オンプレ/クラウド)に侵入されるケースは今後も継続する
- メール経由で拡散する別種のマルウェア(Emotet等)からの被害が日本国内でも増加する
- 境界防御が適切に行われている組織でもインシデントが増加する

## 掌握 – より標的型攻撃に近い手法の採用

- 攻撃者の変化に伴い、RATの利用/BloodHound等の攻撃ツールの利用事例が国内でも増加すると予想
- RATが利用されることで、根絶・終息がより困難に
- 一度データを復旧しても、継続的に繰り返し暗号化被害が発生するインシデントが起こりうる

# 2020年及び今後の国内ランサム(ウェア)

## 脅迫 – ファイルの暗号化以外の方法の採用

- 可用性への攻撃

- 全ドメインアカウントのパスワード変更(攻撃者が)
- 各種サーバのファイル削除や設定変更によるシステム稼働の妨害

- 機密性への攻撃

- 知的財産/研究開発情報/個人情報等の機密情報を取得し、公開と引き換えに脅迫を行う事例も日本へ

- 完全性への攻撃

- データベースやファイルの「一部」書き換えによる業務妨害等

# ランサムウェアに標的型攻撃手法を求めているのは間違っているだろうか

## “標的型”？

- 攻撃者は特定の組織を狙って暗号化や金銭の窃取をしているわけではない
  - 広範囲の攻撃の上で、セキュリティが弱く、金銭を多く窃取できそうな組織で被害発生
- 攻撃を断片的に見ると標的型攻撃と同じ手法はあるが、全体的な攻撃の流れとしては独自の特徴がある

## ランサム“ウェア”？

- ランサムウェアは金銭搾取のために脅迫を行うための一つ的手段に過ぎない
  - 金銭に繋がる脅迫方法があれば、ランサム“ウェア”である必要はない
- ランサムウェアに加えて、そこに至るまでの攻撃のプロセス(侵入、掌握)を把握・遮断することがインシデント対応では重要

マルウェア・ツール名	SHA-256 ハッシュ値
NLBrute1.2	E21569CDFAFBBDD98234EF8AFCC4A8486D2C6BA77A87A57B4730EB4A8BD63BC2
NS.exe	F47E3555461472F23AB4766E4D5B6F6FD260E335A6ABC31B860E569A720A5446
KPortScan3	080C6108C3BD0F8A43D5647DB36DC434032842339F0BA38AD1FF62F72999C4E5
SoftPerfect Network Scanner	66C488C1C9916603FC6D7EC00470D30E6F5E3597AD9F8E5CE96A8AF7566F6D89
MS16-032	9F023D74CF5E16A231660805ADFC829C1BE24A6B1FA6CB3ED41F0E37FE95062B 9AFAE820C8F7ED5616A4523A45968CFDABF646C5151A9C1DB1A6E36D7A9D1E11
rsa.exe	48303E1B50B5D2A0CC817F1EC7FA10C891F368897B0AEA2D02F22701D169CE54 E6CCB71FD62783DE625CBFCDAE1836B9FFB33B0E2344D709F5B6C5B2E6EAC8D8
mRemoteNC	3BC3038749427E1D6DA05FD3972A86F3403B40102974BD241A233EBD2C3B8C5C
mRemoteNG	9476FE1896669163248747785FA053ACA7284949945ABD37C59DAE4184760D58
Ammy Admin	5FC600351BADE74C2791FC526BCA6BB606355CC65E5253F7F791254DB58EE7FA A0C996178FAA8320948D886F47EF394C712F1E5DC0F7C8867CD4BB1DB5F2A266
xDedicLogCleaner	878706CD11B5223C89AAEF08887B92A655A25B7C630950AFFA553574A60B922E
Advanced IP Scanner	02EC949206023F22FE1A5B67B3864D6A653CC4C5BFCB32241ECF802F213805E8
PCHunter	D1AA0CEB01CCA76A88F9EE0C5817D24E7A15AD40768430373AE3009A619E2691

Secureworks®