



Much Ado About Ransomware


NCFI Keynote

11 October 2021

RJ_CHAP

RYANCHAPMANJ

RJ_CHAP

- 10 Years in DFIR
- Principal IR Consultant @ BlackBerry
- SANS Instructor & Author
 - [FOR528](#): Ransomware for Incident Responders
 - FOR610: Reverse Engineering Malware
- Lead Organizer for 
- <https://incidentresponse.training>
 - IRT Consulting LLC



Agenda

The Ransomware Evolution

Ransomware Campaign Overview

Ransomware Infection Vectors (IVs)

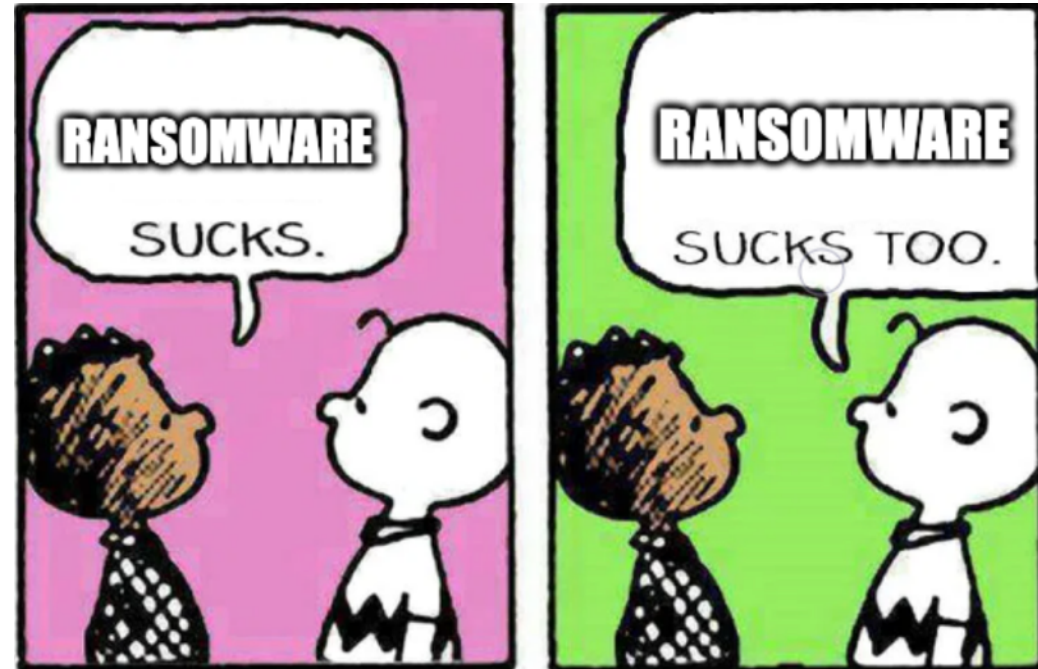
How LE Can Help

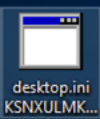
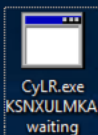
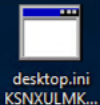
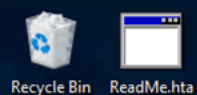
Your Tasks, Should You Choose to Accept Them

Wrap-Up

Ransomware Sucks

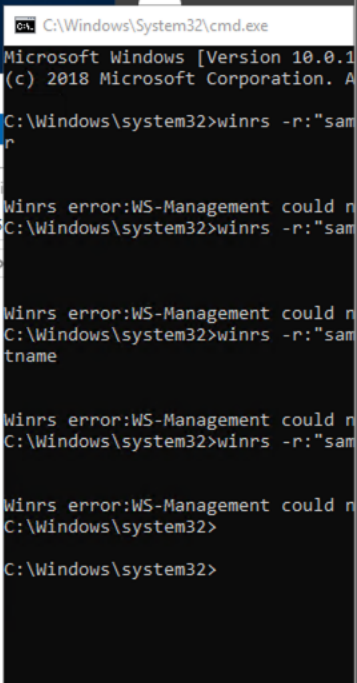
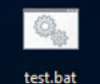
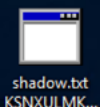
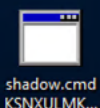
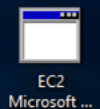
- These groups are persistent
- They DON'T CARE
- Their job is *easy*
- Our job is difficult
- They keep learning
- The royal “we”... don't
- They win, because we falter
- #RansomwareSucks








desktop.ini KSNXULMK...
Type: WAITING File
Size: 1.77 KB
Date modified: 9/10/2021 7:09 AM

Feedback.w...





YOUR FILES ARE ENCRYPTED

Your PC security is at risk
All your files were encrypted and important data was copied to our storage
If you do not need your files, then the private key will be deleted within 5 days
If you want to restore files and return important data, application, contact the operator and enter YOUR ID **KSN** 
ID of your personal operator **57309B4FFB75** 
If the Operator did not respond within 24 hours or encountered any problem then send an email to our support massons81@aol.com
In the header of the letter, indicate your ID and attach 2-3 infected files for the decryption tool
Files should not have important information and should not exceed the size of more than 5 MB
As our guarantees, we will return your files restored

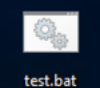
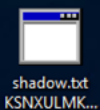
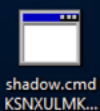
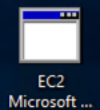
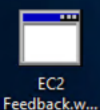
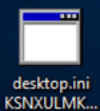
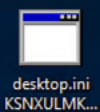
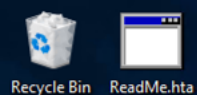
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

4:06:16:17

Hostname: samaran-dc
Instance ID: i-0e0ef2b...
Private IP Address: 10...
Instance Size: m4.large
Availability Zone: us-east-2a
Architecture: AMD64
Total Memory: 8192 MB
Network Performance: Moderate





uTox (Alpha) (version : 0.14.0)

uTox User

Toxing on uTox, from th...

All Contacts

Create Groupchat

Right click

Search/Add Friends

ReadMe.hta

test.bat

test2.bat

uTox Settings

Profile | User Interface | Audio & Video | Notifications | Advanced

Name

uTox User

Status Message

Toxing on uTox, from the future!

Tox ID

Copy

1E8331D58579f...

Language

English

Hostname: samaran-dc
Instance ID: i-0e0ef2b...
Private IP Address: 10...
Instance Size: m4.large
Availability Zone: us-east-2a
Architecture: AMD64
Total Memory: 8192 MB
Network Performance: Moderate

ARE ENCRYPTED

contact the operator and enter YOUR ID KSN...

AF220...

send an email to our support massons81@aol.com

decryption tool

re than 5 MB

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

4:06:40:33

Windows taskbar with icons for Start, Search, Task View, and several open applications. System tray shows the time as 5:19 PM on 9/10/2021.

It All Began With...

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

AJ_CHAP

Evolution of Ransomware

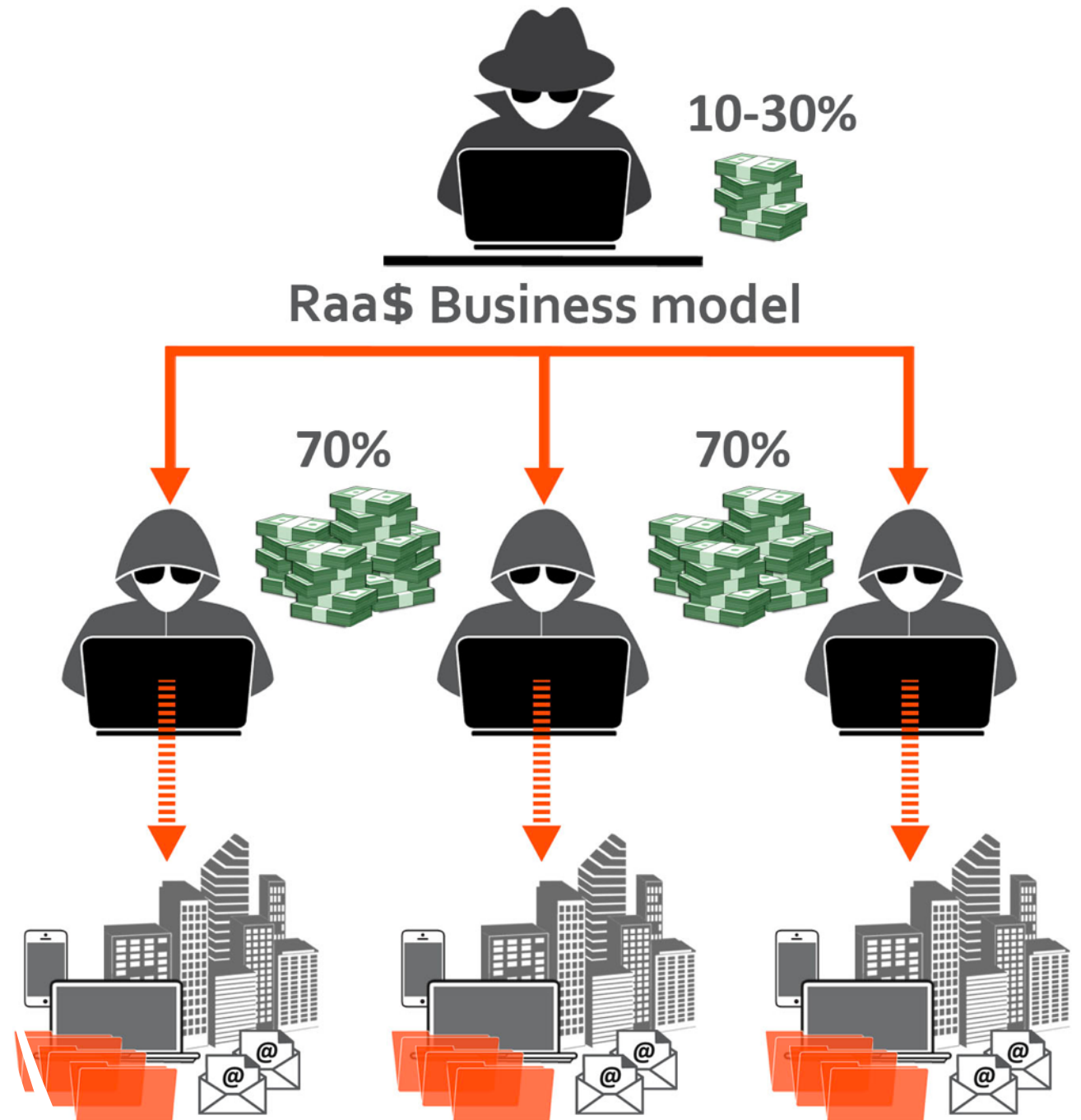


HUMOR → RaaS

- And then things got ugly
- Human-Operated Ransomware (HUMOR)
 - Distribution through hands on keyboard
 - Enables enterprise-wide distribution
- Ransomware-as-a-Service (RaaS)
 - Enables *anyone* to become an **affiliate**

Ransomware-as-a-Service (RaaS)

- Core groups aren't large
- You'll be dealing with **affiliates**
- Intrusion Access Brokers (IABs)
- Pentesters
- Negotiators
- Money mules



Active Affiliate Recruiting



LEAKED DATA



CONDITIONS FOR PARTNERS AND CONTACTS

[RETURN BACK](#)

**CONDITIONS
FOR PARTNERS**

RJ_CHAP

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM language with no dependencies. Encryption is implemented in parts via the completion port (I/O), encryption ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the work. It is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**
- **launch of computers switched off via Wake-on-Lan;**
- **print-out of requirements on network printers;**
- **available for all versions of Windows OS;**

The Worst Becoming Worse!

Double extortion

Triple extortion

Worse than we are

URL

<https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-leak-data-if-victim-contacts-fbi-police/>

Details_

Few days ago [one group posted interesting thoughts](#) about the situation here.

We'd like to make some comments and maybe extend some thoughts from our point of view.

Police, FBI and Recovery Company™. Who cares about the data in a ransom case?

But answer is too simple to be truth: 2 sides are interested.

One side is company affected. Second side is ransom operator. Nobody else.

Also interesting is common reaction in media: [The question is – when your company gets hit by Ragnar Locker, are you going to let them determine the rules or not?](#)

Ofcourse much better way is to pay Recovery Company™ upfront.

And now they determine the rules. But in this rules there is no place for data safety.

It's just a business model where Recovery Company™ earns it's money just because it exists.

They must be significant specialist in recovery. But no, unable to recover most of data without proper backups.

They must be perfect negotiators. But no once again. They just use variations of same script.

Do they interested in solution? And you know the answer: NO. They will get paid either way.

It's also looks like that some of those companies are affiliates of some groups with huge number of targets.

Conveyor for a percentage.

Don't pay ransom. Pay that "good guys". But what for? Would they recover data? Nope. Would they prevent the release of sensitive data? No. And what do they do? They are "good".

We wanna play a game. If we see professional negotiator from Recovery Company™ - we will just destroy the data.

Recovery Company™ as we mentioned above will get paid either way. The strategy of Recovery Company™ is not to pay requested amount or to solve the case but to stall. So we have nothing to loose in this case. Just time economy for all sides.

What will this Recovery Companies™ earn when no ransom amount is set and data simply destroyed with zero chance of recovery? We think as usual - millions of dollars. Clients will bring money for nothing. As usual.

USA	1699
Canada	205
France	176
UK	169
Germany	128
Italy	121
Australia	67
Spain	64
Brazil	61
Japan	42
India	39
Switzerland	33
Mexico	31
Netherlands	22
United Arab Emirates	22
South Africa	21
Taiwan	20
Austria	19
Belgium	17
China	15
Indonesia	15
South Korea	15
N/A	14
Chile	13
Saudi Arabia	13
Argentina	12
Israel	12
Norway	12
Peru	12
Portugal	12
Sweden	12
Thailand	12
Colombia	11
Turkey	11
New Zealand	10
Singapore	10
Hong Kong	9
Czech Republic	7
Ireland	7
Poland	7
Romania	7

Statistics on countries affected by darkweb ransomware

United Arab Emirates

0.7%

Netherlands

0.7%

Mexico

0.9%

Switzerland

1.0%

India

1.2%

Japan

1.3%

Brazil

1.8%

Spain

1.9%

Australia

2.0%

Italy

3.6%

Germany

3.8%

UK

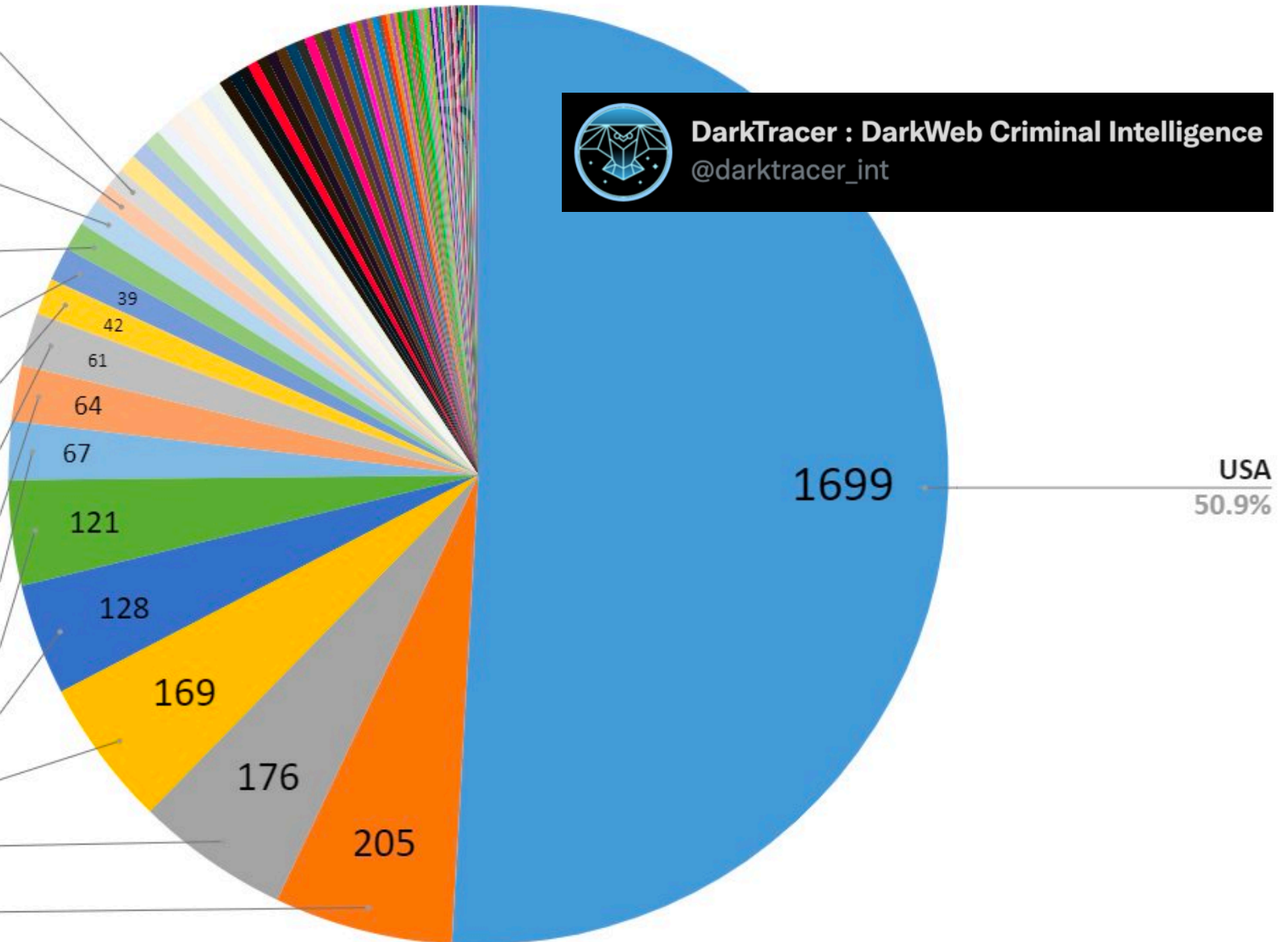
5.1%

France

5.3%

Canada

6.1%



Ransomware Teams Evolving

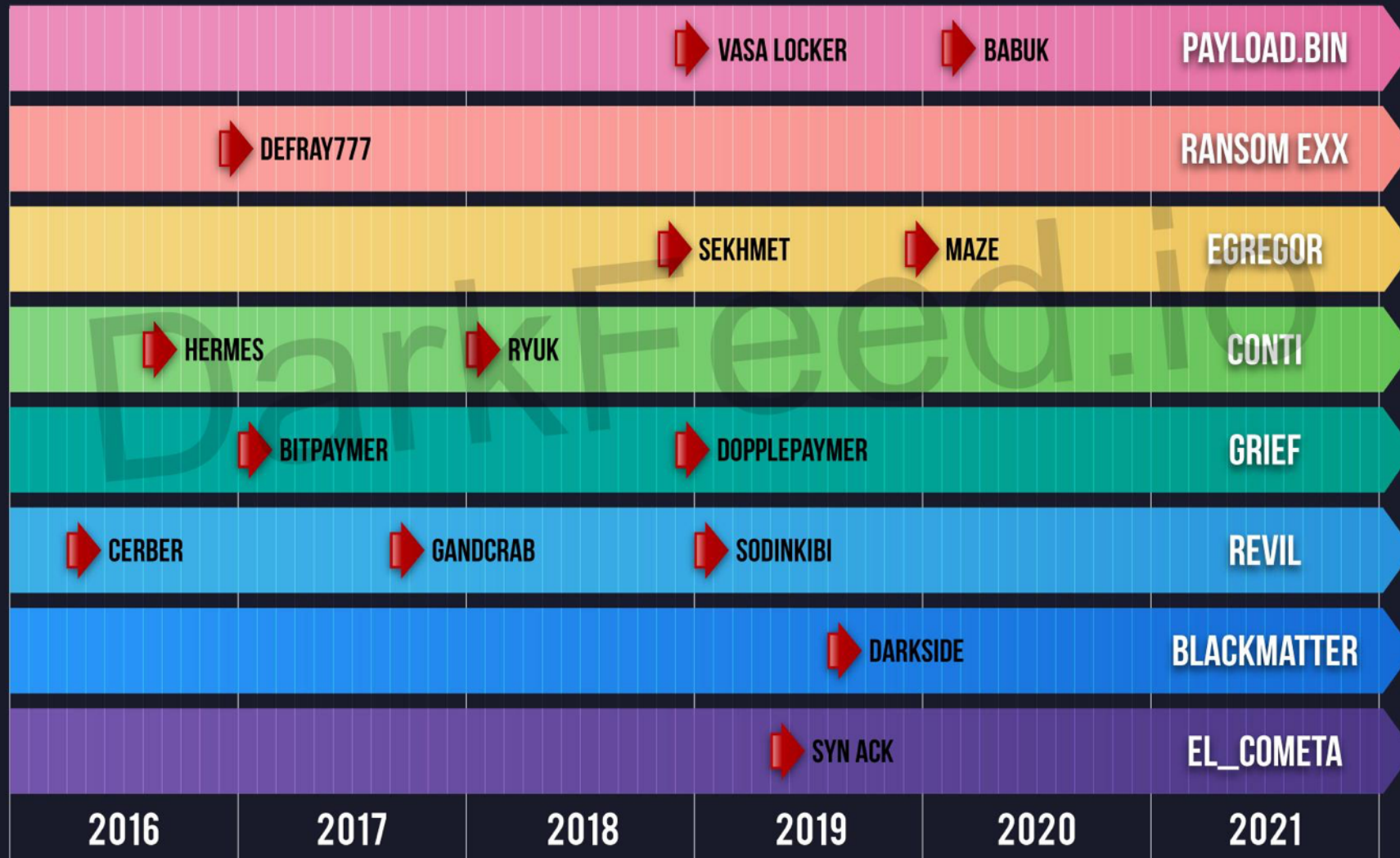
- Teams don't die out easily
- Affiliates move between teams
- Too much heat == "quit"
- Quit == change name 😊
- TTPs often quite similar
- Darkweb intelligence services critical





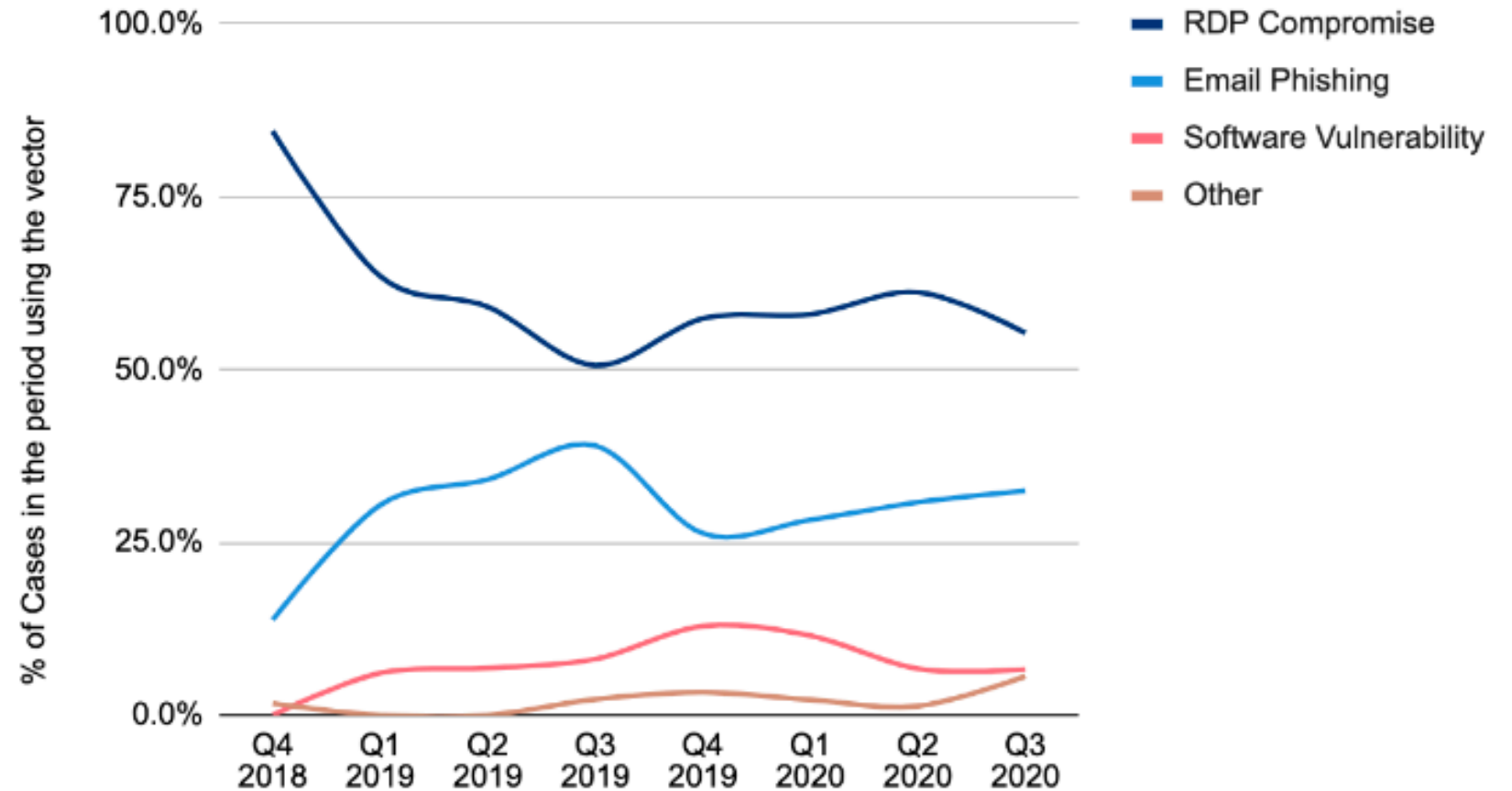
DarkFeed
DeepWeb Intelligence Feed

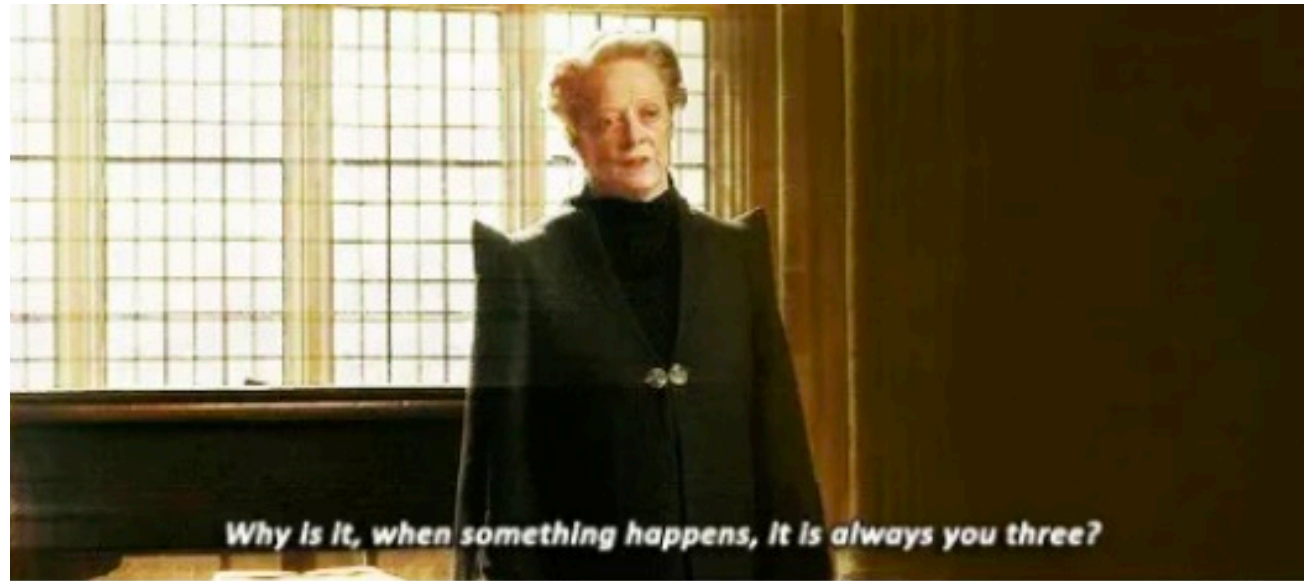
RANSOMAP EVOLUTION



Infection Vectors

Ransomware Attack Vectors





RJ_CHAP

RDP and Phishing Reign Supreme

- Remote Desktop Protocol (RDP) is often #1
- WHY?! No seriously -- WHY?!
 - RDP exposed to the Internet
 - **“We don’t have RDP open to the Internet.”**
- Credential stuffing / spraying / brute-forcing
- Phishing is a %s game
 - It only takes ONE – Just one!
- Measures can be taken to minimize phishing effectiveness
 - e.g. Users != admins

- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8243
- CVE-2019-11539
- CVE-2019-11510

Pulse
Secure VPN



- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-19781
- CVE-2019-11634

Citrix



- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855

Microsoft
Exchange



- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

Fortinet



- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

SonicWall



- CVE-2021-22986
- CVE-2020-5902

F5



- CVE-2020-2021
- CVE-2019-1579

Palo Alto



- CVE-2021-28799
- CVE-2020-36198

QNAP



- CVE-2020-12271

Sophos



- CVE-2019-0604

SharePoint



- CVE-2019-0708

RDP



- CVE-2017-0199

Microsoft
Office



- CVE-2021-21985

vCenter



AJ_CHAP

Intrusion Access Brokers (IABs)

- Heavy reliance on Malware-as-a-Service (MaaS)
 - Banking Trojans have evolved
 - IcedId, Qbot, AzoRult, Hancitor ('member Emotet?!)
- May work directly with affiliates
 - We're in! >> **Your turn**
- May work independently
- Often sell access

Sale, Sale, Sale!!



 Hosts ▼

 RDPs 24

 cPannels 14585

 Shells 3027

 SSH/WHM 0

 0 ▼

0 +

Ticket 0 ▼

AJ_CHAP

Country :

All Countries

Hosting :

All

SSL :

All

TLD :

Type :

All

Seller :

All

Seo Filter :

Default

Show

100

 entries

Search:

ID	Country	Type	TLD	Hosting	Ip Blacklist	Seo Info	Source	Seller	Check	Price	Added on	Send Test	Buy
38078	 Indonesia	 https	.id		<div>CHECK BLACKLIST</div>	<div>i SEOINFO</div>	 cracked	Seller348	<div>CHECK</div>	5.00	26/03/2021 06:44:08 pm	<div>SEND TEST</div>	<div>BUY</div>
48352	 United States	 https	.com	Cloudflare, Inc.	<div>CHECK BLACKLIST</div>	<div>i SEOINFO</div>	 cracked	Seller341	<div>CHECK</div>	5.00	04/05/2021 03:27:48 am	<div>SEND TEST</div>	<div>BUY</div>
24234	 United States	 https	.com	Jumpline Inc	<div>CHECK BLACKLIST</div>	<div>i SEOINFO</div>	 cracked	Seller353	<div>CHECK</div>	3.00	23/02/2021 08:25:31 pm	<div>SEND TEST</div>	<div>BUY</div>
45405	 United States	 https	.com	WEBSITEWELCOME.COM	<div>CHECK BLACKLIST</div>	<div>i SEOINFO</div>	 cracked	Seller311	<div>CHECK</div>	3.00	25/04/2021 03:49:30 pm	<div>SEND TEST</div>	<div>BUY</div>
39049		 https	.com		<div>CHECK BLACKLIST</div>	<div>i SEOINFO</div>	 cracked	Seller309	<div>CHECK</div>	5.00	27/03/2021 08:23:15 pm	<div>SEND TEST</div>	<div>BUY</div>



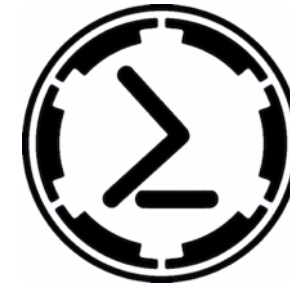
CONTI NEWS

If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

[Web mirror](#)[Tor mirror](#)

A Paradigm Shift

- Over the past 5-6 years
- TAs have become reliant on red teaming tools
- Open source frameworks have taken over
- Heavy reliance on [LOLBAS](#)
- “Dual Use” tools help avoid detection
- [Cobalt Strike](#) readily available to TAs



AJ_CHAP

Activity
другое

TopFuel

T?F



User

87

900 posts

Joined

05/26/17 (ID: 79661)

Activity

другое / other

Posted June 8

Report post

On 6/8/2021 at 3:40 PM, pushclouds said:

Перезаляйте плз у кого осталось

Перезалив CobaltStrike.

Cobalt Strike - разные версии:



Cobalt Strike 4.0 Crack: anonfiles.com/...0-Fixed_zip (4.0-Fixed_zip)

Cobalt Strike 4.0 Source Code: anonfiles.com/...CobaltStrike-master_zip | github.com/Freakboy/CobaltStrike

Cobalt Strike 4.1 Crack: anonfiles.com/...obaltstrike_4.1_rar

Cobalt Strike 4.2 + Toolkits: anonfiles.com/...CS_4.2_rar | pass: Z3R0%oFf

Cobalt Strike 4.2 - ломаная версия с raida: anonfiles.com/...Cobalt_Strike_4.2_zip

Cobalt Strike v 4.3: anonfiles.com/...CS4.3_zip

Cobalt Strike 4.3 cracked final: anonfiles.com/...cs4.3_cracked_final_rar | зануск teamserver_win.bat 127.0.0.1 sUp3r@dm1n | порт для клиента 50050 pass: sUp3r@dm1n

Cobalt Strike - Plugins & Toolkits: anonfiles.com/...CS_Plugins_Toolkits_rar

ps: на склейки не проверял - тестируем сами.



Quote

2



AJ_CHAP

Attack Overview DEMO

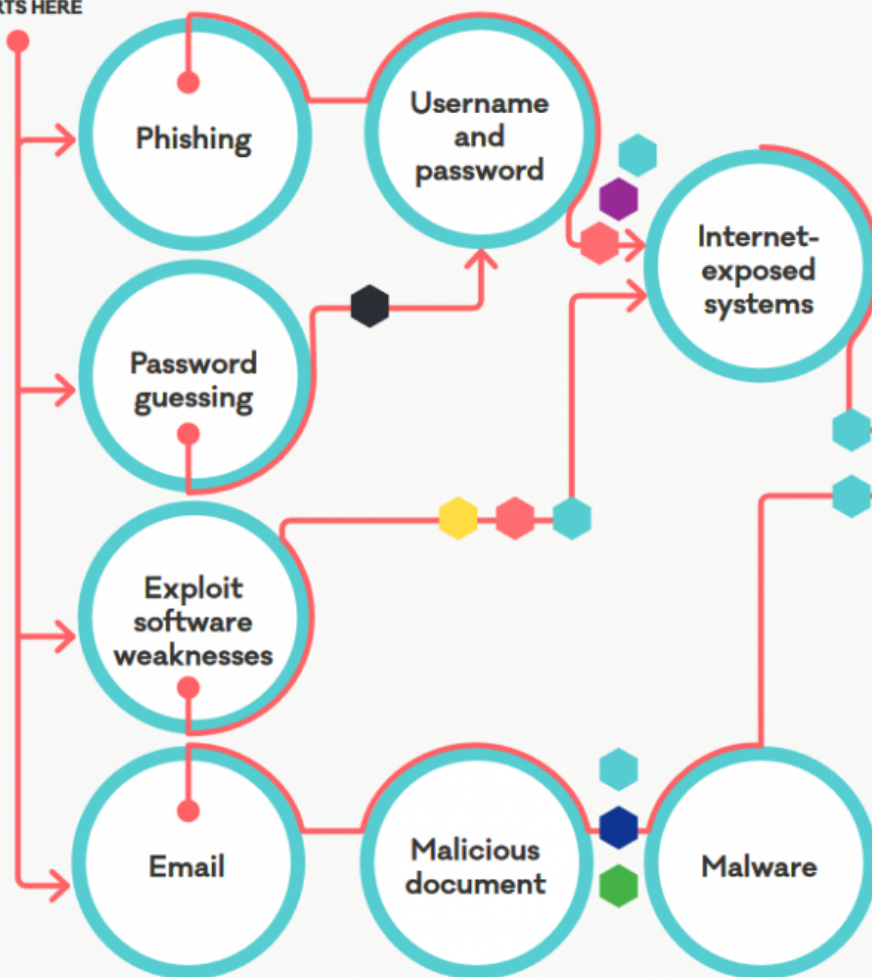
- [PYSA/Mespinoza Ransomware](#)



INITIAL ACCESS

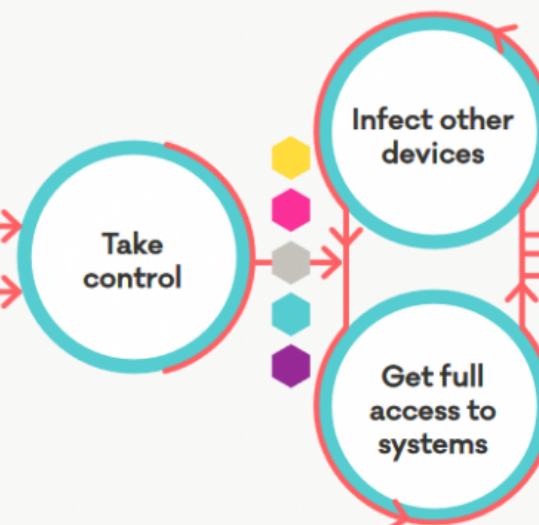
Attacker looks for a way into the network

ENTRY FOR
ATTACK
STARTS HERE



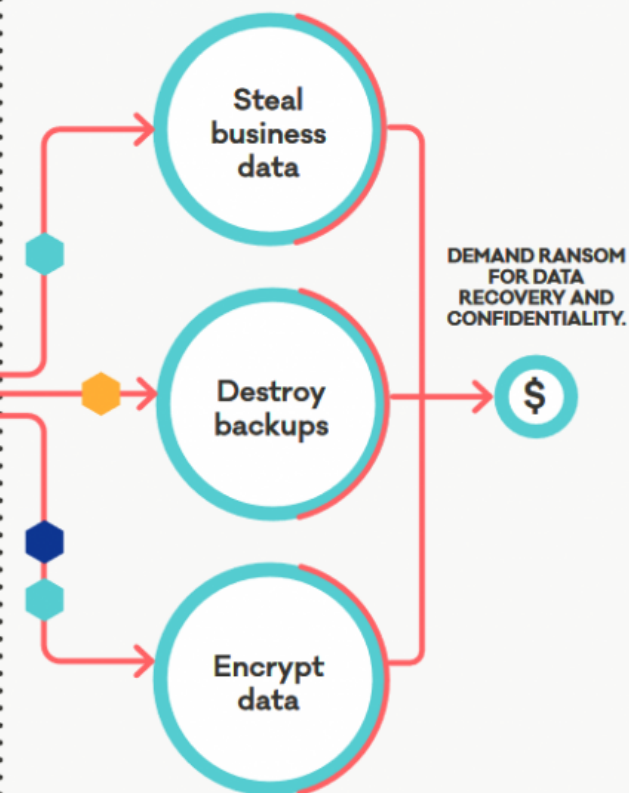
CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices



IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom



Talk to your IT provider about the relevant CERT NZ Critical Controls for your business.

CRITICAL CONTROLS KEY



Internet-exposed services



Patching



Multi-factor authentication



Network segmentation



Principle of least privilege



Backups



Application allowlisting



Logging and alerting



Disable macros



Password manager



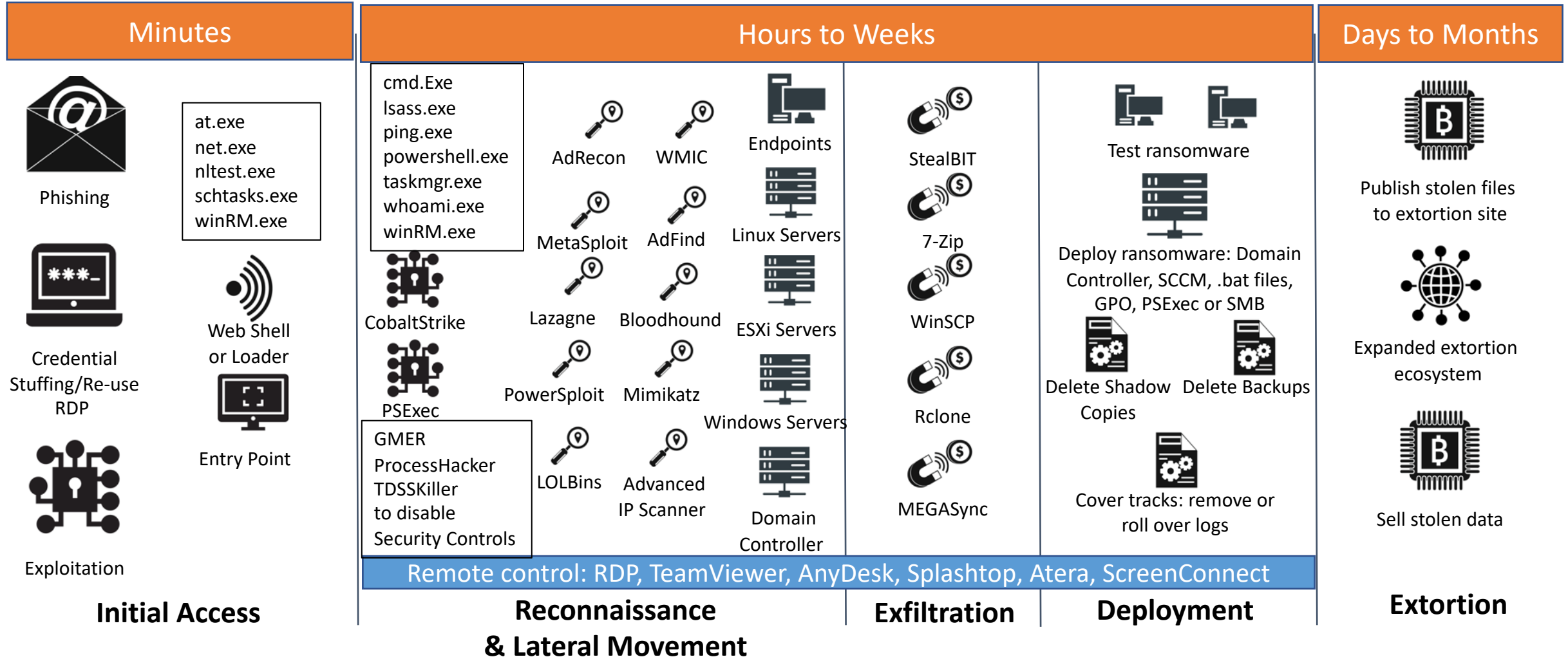
Compromised
Redirect Infrastructure



Real C2
Infrastructure



Extortion Site



RF Conti Pentester Guide Leak | Re X

GitHub - ForbiddenProgrammer X

+


https://raidforums.com/Thread-Conti-Pentester-Guide-Leak?highlight=conti+leak

Conti Pentester Guide Leak

by ramosidi04 - August 15, 2021 at 10:02 PM

New Reply

ramosidi04



Uber User

Posts	321
Threads	49
Joined	Jan 2021
Reputation	20

August 15, 2021 at 10:02 PM

#1

Conti Pentester Guide Leak

Link: <https://github.com/ForbiddenProgrammer/c...guide-leak>

This repository was created to archive leaked leaked pentesting materials, which were previously given to Conti ransomware group affiliates

Mentioned materials covers topics such us:

- configure the Rclone software with a MEGA for data exfiltration
- configure the AnyDesk software as a persistence and remote access solution into a victim's network
- elevate and gain admin rights inside a company's hacked network
- take over domain controllers
- dump passwords from Active Directories
- connect to hacked networks via RDP using a Ngrok secure tunnel
- install the Metasploit pen-testing framework on a VPS
- brute-force routers, NAS devices, and security cameras
- configure and use the Cobalt Strike agent
- perform a Kerberoasting attack
- use the NetScan tool to scan internal networks
- disable Windows Defender protections
- delete shadow volume copies
- configuring operating system to use the Tor and more

Leaked content will give you more insight into how ransomware operators perform their attacks. Futhermore, you can improve your own pentesting skills. Defenders will also benefit from this - you can more eaisly detect and block Conti affiliates attacks.

NOTE: Archive containing CobaltStrike crack was removed to please GitHub's Terms of Service.

NOTE2: Materials are written in Russian language (however, due to misspells, threat actor is believed to be Ukrainian citizen)

NOTE3: If something requires password, try "xss.is"

PM Find

Reply Quote Report

Conti Leak DEMO

RJ_CHAP

LE's Role

- Often work with SMBs
- Identify the ransomware family/group
- Identify encrypted systems
- Identify data exfiltration (“exfil”)
- Identify the Infection Vector
- Consulting for system/network restoral

The Outlook is Hazy

- No EDR
- No SIEM
- No PCAP
- Little/no firewall logging
- No extensive logging
 - Logs have rotated
- Few if any security products/appliances



A Matter of Evidence

- DISCUSSION:
 - What can or do you gather?
 - What can or do you analyze?
- How do you collect in bulk?
- How do you analyze in bulk?

Artifacts of Interest

- NTFS artifacts
 - \$MFT
 - \$UsnJrnl:\$J
- Windows Event Logs
 - EVTX files (if not aggregated)
- Registry hives

Collecting Artifacts

- Forensic imaging is slow
 - Useful for finding deleted files
- Triage collection is key
- Triage collection frameworks:
 - [KAPE](#)
 - [CyLR](#)
 - [Kansa](#)
- Triage data can be reviewed in EnCase / Axion / X-Ways / etc.

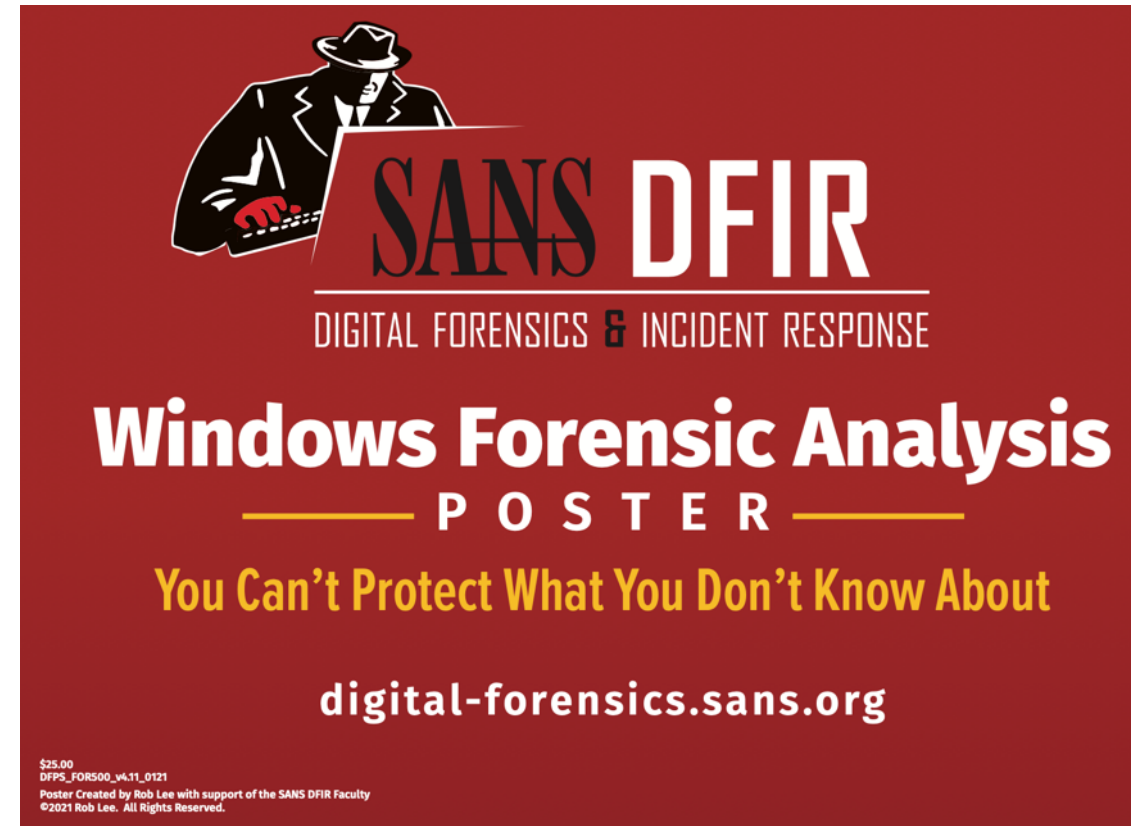


Ingesting Artifacts at Scale

- log2timeline / Plaso
- Elasticsearch, Logstash, & Kibana (ELK)
- Timesketch
- See: [SKADI](#)
 - Pro: Fantastic example of an ecosystem
 - Con: Project has been archived by the owner
 - (i.e. Don't deploy and depend on this, rather learn from it)

Identifying Execution

- [“Windows Forensic Analysis” poster](#)
 - Requires a free SANS login



Identifying Encryption

- Ransomware announces itself
- File suffixes usually easy to identify
- Each family has its own suffixes
 - Sometimes random
- Review service-related Event IDs
 - Event IDs 7034-7036, 7040, 7045, 4697
- Review task-related Event IDs
 - 4698
 - 106, 140/1, 200/1

Identifying Data Exfil

- \$MFT and \$UsnJrnl:\$J **extremely** useful
- Search for archives created
 - e.g. “.zip” and “.rar” archives
- Check for signs of rclone (inc. rclone.conf)
- Review firewall logs for cloud sharing sites
 - ANYTHING not common/approved
 - MEGA very common
- FileZilla & WinSCP
- PowerShell scripting (4103/4104 logs, if available)

Identifying the IV

- Timeline creation critical
 - Compromised accounts lead to initial host(s)
- Review email security gateway logs
- Review [Trusted Documents](#)
- Remote Desktop Protocol Event IDs
 - 4624/5
 - 4778/9
 - 1149
 - 21-25

The Road to Recovery

- Any machine impacted should be rebuilt
- Are backups available?
- Are backups available *prior to infection date*?
 - **Use backups taken well before the infection date**
- User machines should be rebuilt if possible

Final Thoughts

- Ransomware isn't "sophisticated"
 - Group TTPs are well-known
 - Attacks often successful due to poor security posture
 - LE will encounter low visibility
 - Making the best of your visibility == success
-
- **The more public + private sector work together, the better!**

Questions / Comments

- I'd love to hear from YOU!
- Twitter: [@rj_chap](https://twitter.com/rj_chap)
- LinkedIn: [linkedin.com/in/ryanjchapman](https://www.linkedin.com/in/ryanjchapman)
- **Questions / Comments?**