Mikroceen: Spying backdoor leveraged in high-profile networks in Central Asia

welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia

May 14, 2020

ESET researchers dissect a backdoor deployed in attacks against multiple government agencies and major organizations operating in two critical infrastructure sectors in Asia

Peter Kálnai
14 May 2020 - 02:00PM

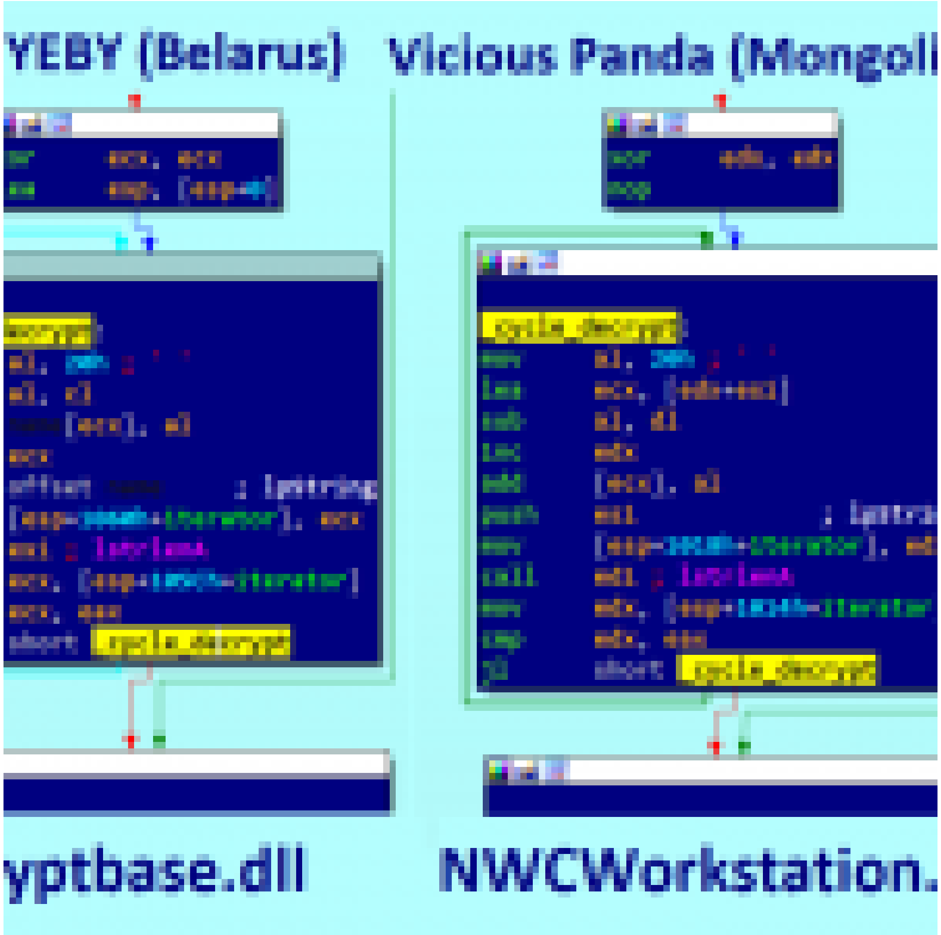
ESET researchers dissect a backdoor deployed in attacks against multiple government agencies and major organizations operating in two critical infrastructure sectors in Asia

In this joint blogpost with fellow researchers from Avast, we provide a technical analysis of a constantly developed RAT that has been used in various targeted campaigns against both public and private subjects since late 2017. We observed multiple instances of attacks involving this RAT, and all of them happened in Central Asia. Among the targeted subjects were several important companies in the telecommunications and gas industries, and governmental entities.

Moreover, we connect the dots between the latest campaign and three previously published reports: Kaspersky's Microcin against Russian military personnel, Palo Alto Networks' BYEBY against the Belarussian government and Checkpoint's Vicious Panda against the Mongolian public sector. Also, we discuss other malware that was typically a part of the attacker's toolset together with the RAT. We chose the name Mikroceen to cover all instances of the RAT, in acknowledgement of Kaspersky's initial report on the family. The misspelling is intentional, in order to avoid the established microbiological notion, but also to have at least phonemic agreement.

Clustering

First let's discuss the clustering of Mikroceen, which is a simple RAT, and show our reasons for thinking reports from Kaspersky, Palo Alto Networks and Checkpoint write about the same specific malware family (among other malicious tools mentioned). Figure 1 provides a comparison of the decryption loop that is used for configuration data consisting of the C&C domain, a name and a password associated with each sample of the RAT. The loop is practically the same and it is implemented in three copies in a row. Checkpoint also discussed the similarities of the HTTP headers in the data sections between BYEBY and Vicious Panda, and a shared logging message V09SS0IO that base64 decodes to WORKIN. The encoded string is also present in Microcin.



```
xor     edx, edx
nop

cycle_decrypt:
mov     al, 20h ; ' '
lea     ecx, [edx+esi]
sub     al, dl
inc     edx
add     [ecx], al
push    esi             ; lpStri
mov     [esp+[illegible]+iterator], ed
call    edi ; lstrlenA
mov     edx, [esp+[illegible]+iterator
cmp     edx, eax
jl      short cycle_decrypt
```

Figure 1. Part of the code used to decipher internal data; the exported DLL name is at the bottom

In the section *Attackers' arsenal* below we also compare the command grammars of the RAT's features and typical error messages that are logged during execution with its previous instances. To support the evidence, the preferred provider of the attackers' infrastructure and the most typical malware simultaneously found on the compromised networks. All these clues should evoke strong confidence that it's the same malware family.

Timeline & victimology

Figure 2 sketches the evolution how the threat was tracked in time. As we mentioned earlier, the Central Asian region joined Russia, Belarus and Mongolia as areas with victims of Mikroceen intrusions. These victims were not desktop users, but endpoints in corporate networks where a higher level of security is expected.

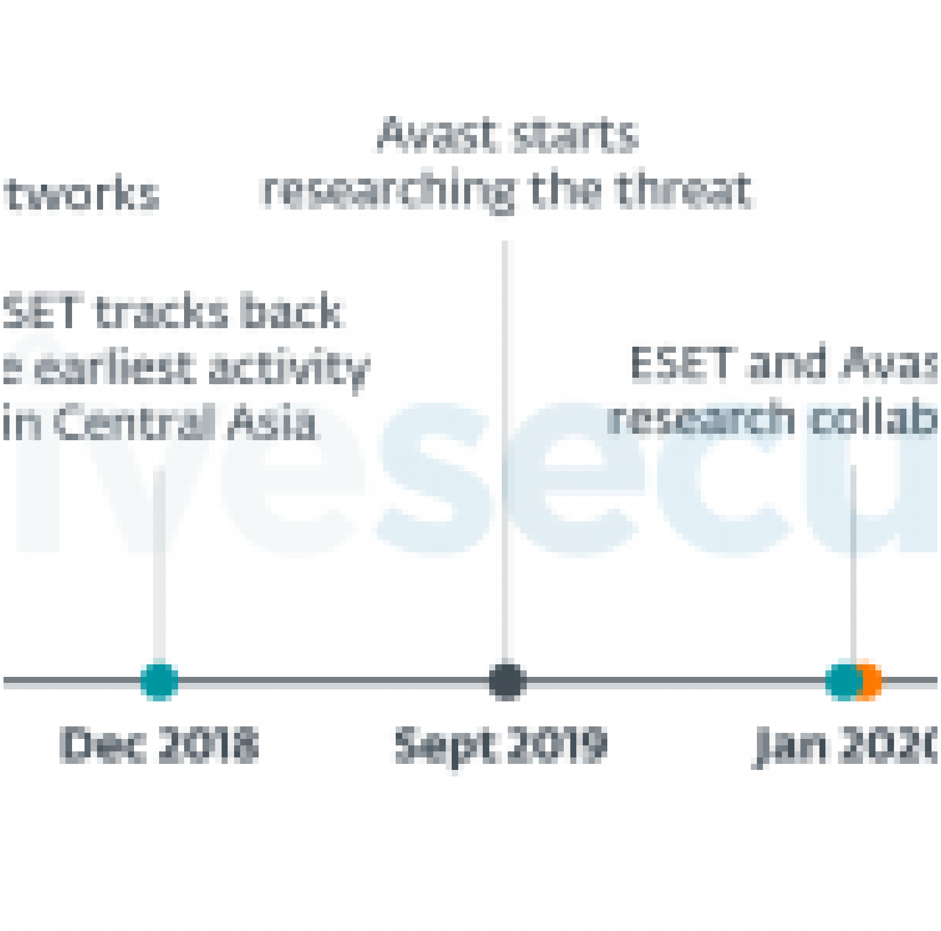

tworks
Avast starts researching the threat
SET tracks back e earliest activity in Central Asia
ESET and Avas research collab
Dec 2018
Sept 2019
Jan 202(

Figure 2. Timeline of events related to Mikroceen

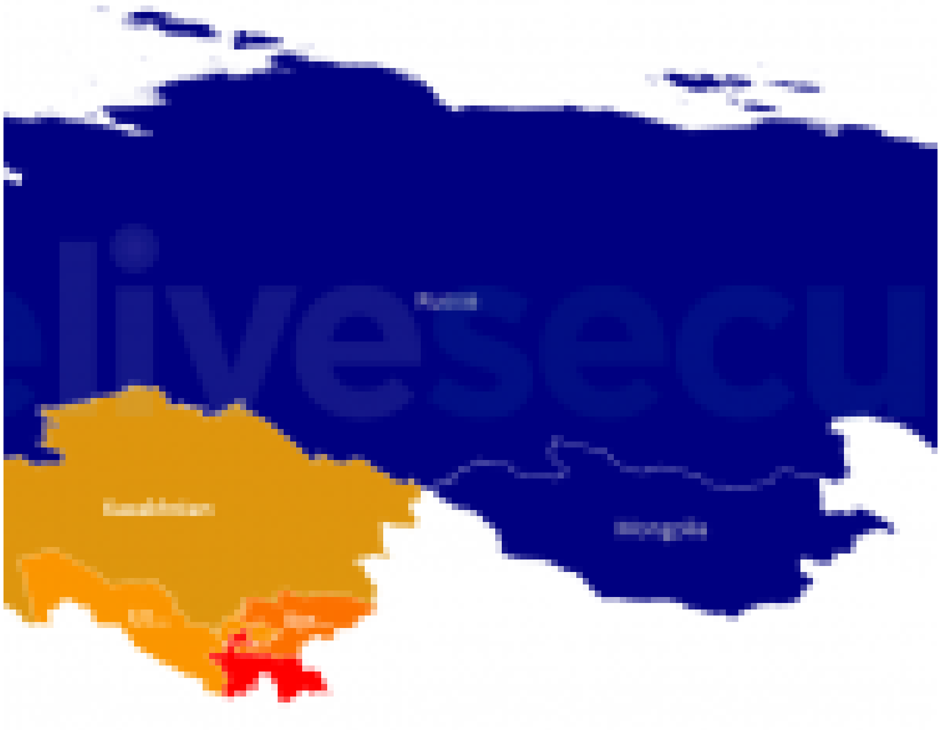


Figure 3. The recent campaigns in Central Asia surrounded by the previously reported ones

Attackers’ arsenal

Let us describe the tools the attackers used in their campaign in Central Asia. Unfortunately, we were unable to discover how they got into the compromised networks.

RAT (client-side backdoor)

Once the intruders establish a foothold on a victim machine, the code in Figure 4 serves to install the RAT on the system. Note the parameter start= auto, which establishes the malware’s persistence after a reboot.

```
@echo off
sc stop PCAudit
sc delete PCAudit
sc create PCAudit binpath= "C:\WINDOWS\syswow64\svchost.exe -k netsvcs" type= share start= auto displayname= "Windows Upload Manager"
sc description PCAudit "Windows Help Service is a microsoft Windows component for System(Important). If this service is stopped, users will be unable to get useful information"
sc failure PCAudit reset= 0 actions= restart/0
reg add HKLM\SYSTEM\CurrentControlSet\Services\PCAudit\Parameters /v ServiceDll /t REG_EXPAND_SZ /d %SystemRoot%\Syswow64\pcaudit.dll
reg add HKLM\SYSTEM\CurrentControlSet\Services\PCAudit\Parameters /v ServiceMain /t REG_SZ /d NtHelpServiceMain
reg add HKLM\SYSTEM\CurrentControlSet\Services\PCAudit\Parameters /v ServiceDllUnloadOnStop /t REG_DWORD /d 1
sc start PCAudit
del %0
```

Figure 4. Installation batch code

As we mentioned earlier, each bot comes with configuration data: C&C, client name and client password. The name of the bot appears in the server-side interface. What is quite unusual is that an operator needs to authenticate by entering the client's password in order to control the client. We can only speculate about the purpose, but it could serve as protection against botnet takeover, in case a competing actor or law enforcement seize their infrastructure. So, we see that certain effort was put on the security of the client-server connection. Moreover, the client can connect directly to the C&C server or route the traffic via a proxy, which could be useful – especially in corporate networks. The connection is further secured by a certificate and this is a feature that distinguishes Mikroceen from the legion of backdoors we have seen since previously.

Mikroceen uses the same basic features as already described Palo Alto Networks about BYEBY. The grammar of commands is quite specific, because each command is truncated to 6 letters and then base64 encoded. That results an 8-letter incomprehensible word in the code. While in previous cases the encoding was straightforward, in the campaign in Central Asia there's additional unknown encryption layer added. The connection of the 8-letter words with the commands in that case was done by agreement on the code level.

Command	Microcin, BYEBY, Vicious Panda	Mikroceen
hello!	aGVsbG8h	AmbZDkEx
GOODBY	R09PREJZ	eYTS5IwW
BYE BY	QllFIEJZ	bo7aO8Nb
DISCON	REITQ09O	6GEI6owo
LIST D	TElTVCBE	Ki0Swb7I
STARTC	U1RBUlRD	h71RBG8X
COMMAN	Q09NTUFO	5fdi2TfG
TRANSF + (UPLOAD, DOWNLO)	VFJBTlNG + (VVBMT0FE, RE9XTkxP)	J8AoctiB + (QHbU0hQo, hwuvE43y)
EXECUT	RVhFQ1VU	gRQ7mIYr

Table 1. Command grammar of various instances of the RAT

During execution, the client logs debug messages in a temporary file. This varies among various Mikroceen instances. Table 2 provides a comparison of these messages from case to case and gives additional evidence that links the instances of Mikroceen.

	Microcin	BYEBY	Vicious Panda	Mikroceen	
				32-bit	64-bit
Folder	% CSIDL_COMMON_DOCUMENTS%	%TEMP%	% CSIDL_COMMON_DOCUMENTS%	%TEMP%	%TEMP%
Filename	7B296FB0.CAB	vmunisvc.cab	5E8C6FF0.CAB	7B296FB0.CAB	W52G86ST.TMP
Keywords at main	V09SS0lO U3RhcnQ=	V09SS0lO U3RhcnQ=	V09SS0lO U3RhcnQ=	V09SS0lO	GvFa8Sei
Keyword at connect	ZGlyZWN0	ZGlyZWN0	ZGlyZWN0	wfZ155bJ	wfZ155bJ

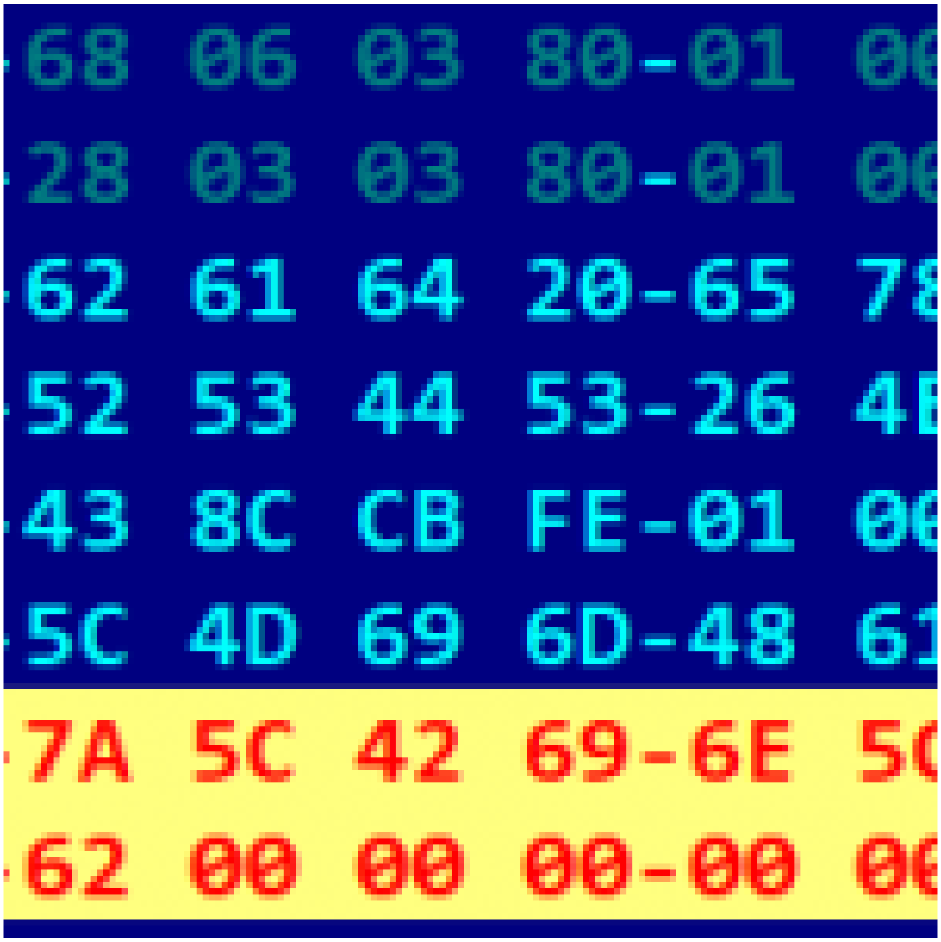
Table 2. Logging messages in a temporary file

Simultaneously occurring malware

The previous reports always mention a wide arsenal of tools that are used in the attacks. In our case it was the same – not just Mikroceen, but other malware as well. Here are the three most important tools we observed in the compromised networks.

Lateral movement via Mimikatz

The attackers used their implementation of Mimikatz, delivered via a two-stage mechanism: the first stage was a dropper usually called installer.exe or Yokel64.exe*,* which dropped the main payload with an indicative external DLL name mktz64.dll in the second stage. While Mikroceen has never come with debug information, here we can see the string E:\2018_\MimHash\mimikatz\Bin\mktzx64.pdb



```
68 06 03 80-01 0
28 03 03 80-01 0
62 61 64 20-65 7
52 53 44 53-26 4
43 8C CB FE-01 0
5C 4D 69 6D-48 6
7A 5C 42 69-6E 5
62 00 00 00-00 0
```

Figure 5. A PDB string in the Mimikatz payload

Mimikatz is an open source project by French security researcher Benjamin Delpy, developed since 2007. It's a robust tool that, among other things, can bypass various Windows authentication schemes, basically by dumping credential data from the Windows Local Security Account database. It's mainly used by red teams in IT security but also misused across the spectrum of APT actors, e.g. Lazarus Group, Telebots, Okrum etc. After running it in a test virtual environment, its output is (the incorrect spaces before the commas are in the original):

```
#1 domain = MSEDGEWIN10, user = Administrator , nthash=FC525C9683E8FE067095BA2DDC971889.
#2 domain = MSEDGEWIN10, user = IEUser , nthash=FC525C9683E8FE067095BA2DDC971889.
```

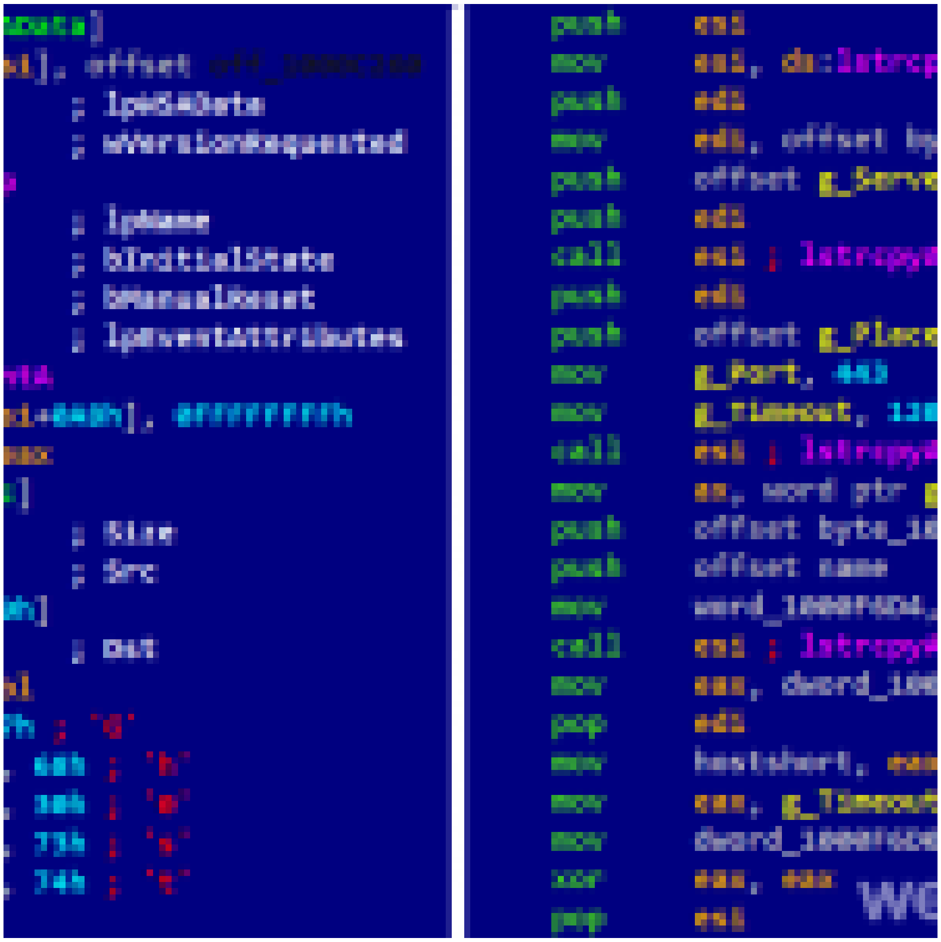
Lateral movement via WMI

The attackers use an additional tool to spread in the hosting network. This time they leverage Windows Management Instrumentation (WMI). All relevant data is needed as the file's name, as during the execution it expects @@<ComputerName>,<UserName>,<Password>,.exe. In the first step, a console to a remote computer is established, where the connection is identified by <ComputerName> and authenticated with (<UserName>, <Password>). Afterwards, proxy security is set to the strict level, which means arguments of each remote procedure call are encrypted and the server's access to local resources is allowed. Then WMI is used again to retrieve the Win32_Process class, which in turn is used to create a process with given parameters. When all the work is done, the tool terminates itself.

Gh0st RAT

This infamous, old RAT was created around 2008. In this instance it was found as rastls.dll on the compromised systems, while the exported DLL name is usually svchost.dll. It tries to connect with https://yuemt.zzux[.]com:443, which resolves to an IP address in China. This is an exception with no explanation, because the server doesn't belong to any of the C&C providers used by Mikroceen. From our point of view, it seems redundant to use this additional backdoor, whose capacity is fully provided by Mikroceen itself.

To recognize this backdoor, one observes the string Gh0st within the binary. The character string uwqixgze} is used as a placeholder for the C&C domain.



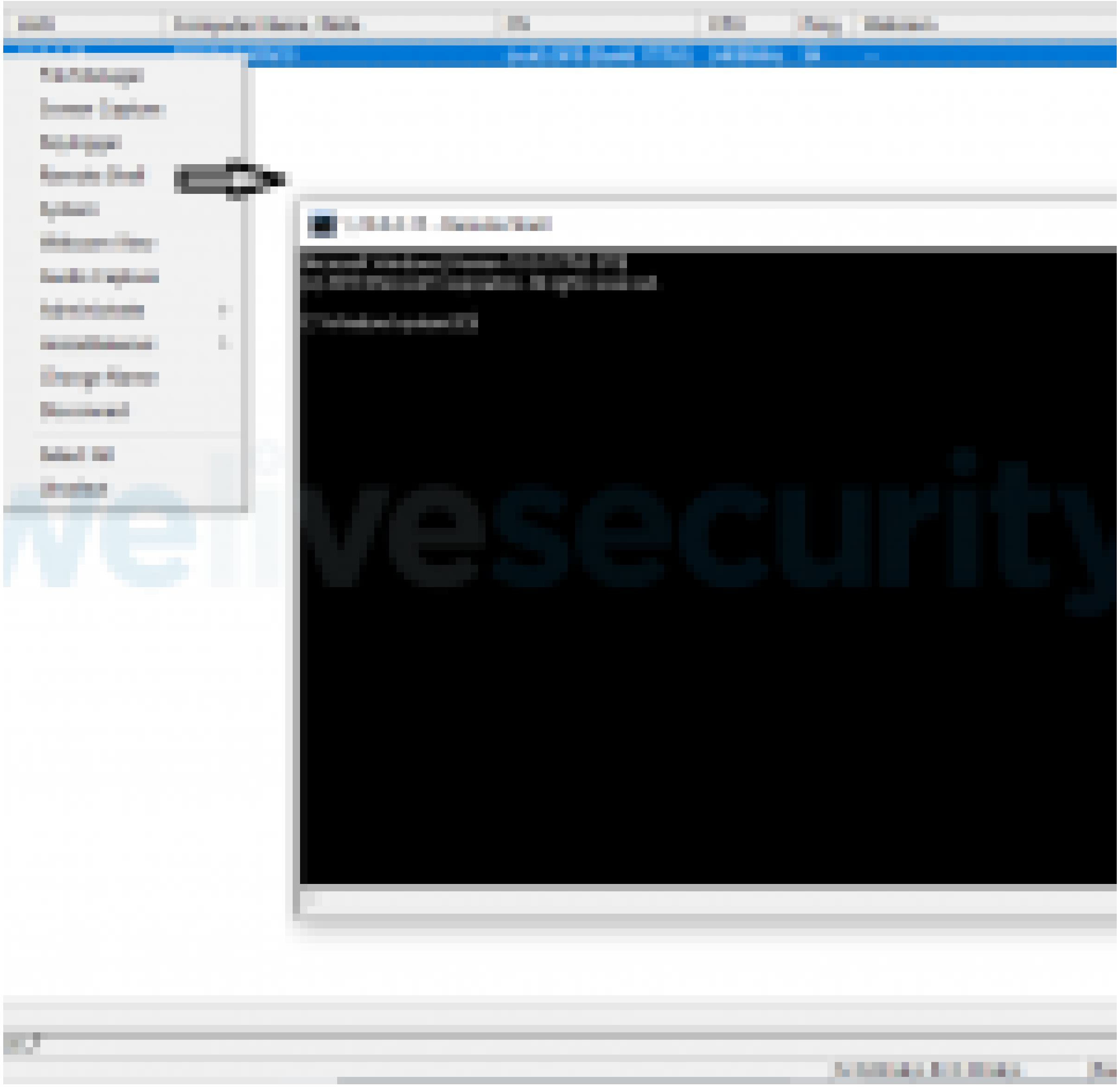
```
Data]
si], offset off_1000C260
        ; lpWSAData
        ; wVersionRequested

        ; lpName
        ; bInitialState
        ; bManualReset
        ; lpEventAttributes
rd4
si+0A0h], 0FFFFFFFFh
eax
x]
        ; Size
        ; Src
h]
        ; Dst
l
h ; 'G'
, 68h ; 'h'
, 30h ; '0'
, 73h ; 's'
, 74h ; 't'
```

```
push    esi
mov     esi, ds:lstrcp
push    edi
mov     edi, offset by
push    offset g_Serve
push    edi
call    esi ; lstrcpyA
push    edi
push    offset g_Place
mov     g_Port, 443
mov     g_Timeout, 120
call    esi ; lstrcpyA
mov     ax, word ptr g
push    offset byte_10
push    offset name
mov     word_1000F5D4,
call    esi ; lstrcpyA
mov     eax, dword_100
pop     edi
mov     hostshort, eax
mov     eax, g_Timeout
mov     dword_1000F5D0
xor     eax, eax
pop     esi
```

Figure 6. Gh0st RAT malware (fragment)

C&C panel (server-side interface)

The previous reports already mention the poor operational security of the attackers (their open directories were observed by Kaspersky and Checkpoint), and the actors behind continue to leak tools not necessarily leveraged on the victims' side. We were able to get our hands on an older version of RAT's control panel. On the lower part of Figure 7 there's a graphical interface through which all bots are commanded. It is very minimalistic, which may be due to an older version from 2017, but still, just compare it with the greater than 10-year-old panel of Gh0st RAT. There's not much improved since, visually or functionally, so the introduction of SSL connections seems like the main shift between the projects (the text box for "CN Name" on the figure). It seems that the operators of the botnet are content customers of Vultr services, a child company of Choopa LLC, as their operational infrastructure is mostly hosted there, and this was also observed in the Vicious Panda campaign by Checkpoint. This is a bullet-proof provider, documented by researchers from Cisco as early as 2015.



```
Microsoft Windows [Version [illegible]]
(c) [illegible] Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

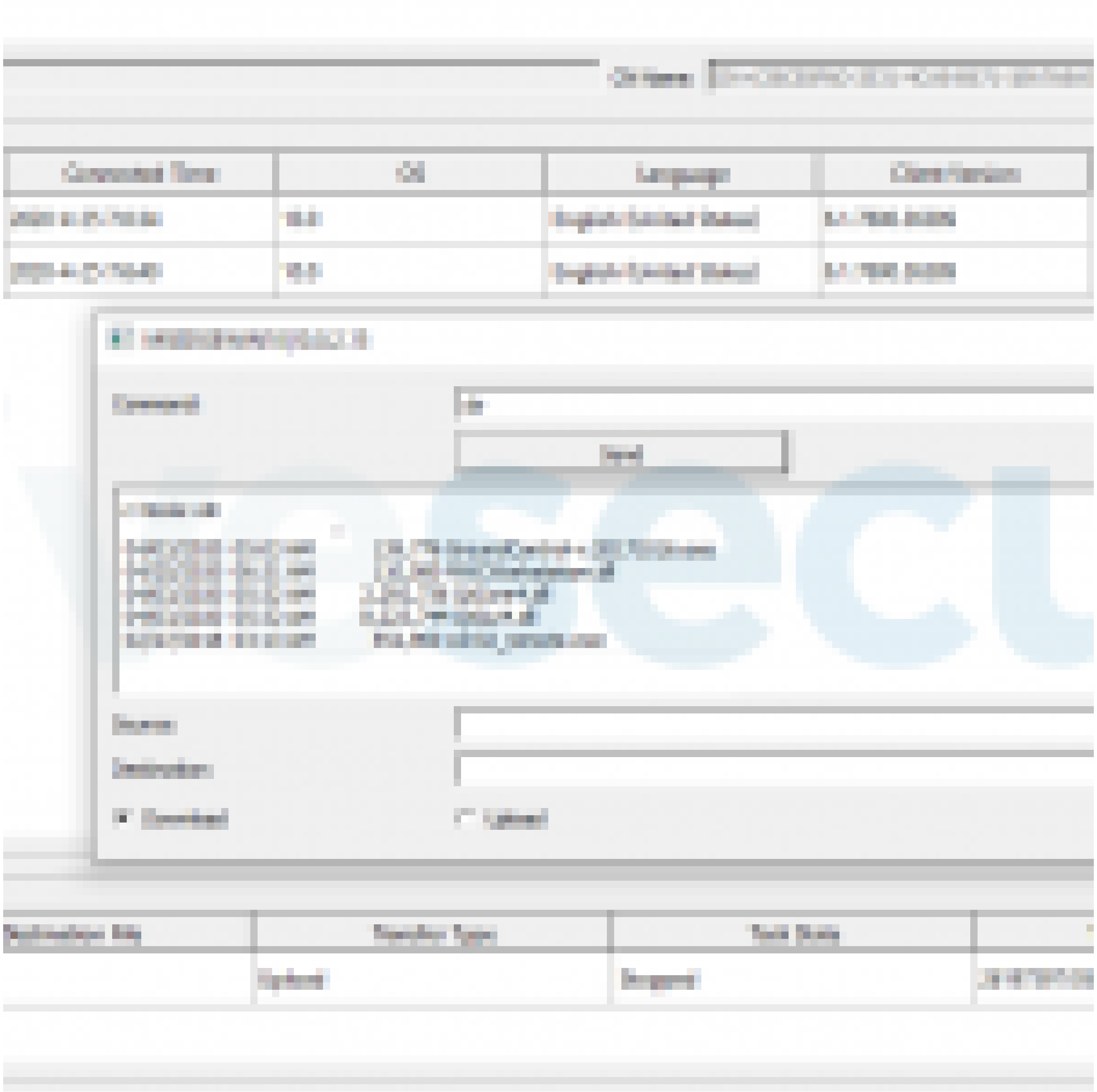


Figure 7. Interfaces for controlling bots: Gh0st RAT (2008) vs. Mikroceen's interface (2017)

Conclusion

We have presented the analysis of a custom implementation of a client-server model developed for spying purposes. The malware developers put great effort into the security and robustness of the connection with their victims and the operators managed to penetrate high-profile corporate networks. Moreover, they have a larger toolset of attack tools at their disposal and their projects are under constant development, mostly visible as variations in obfuscation.

Indicators of Compromise (IoCs)

Here are the hashes of samples described in the article. Additional IoCs collected from the attacks can be found on ESET's GitHub or Avast's GitHub.

SHA	Timestamp	Description
d215bb8af5581b31f194248fc3bd13d999a5991c	2016-06-29 00:34:42	Microcin (Kaspersky) 7771e1738fc2e4de210ac06a5e62c534
7a63fc9db2bc1e9b1ef793723d5877e6b4c566b8	2017-07-06 08:15:31	BYEBY (PANW) 383a2d8f421ad2f243cbc142e9715c78f867a114b037626c2097cb3e070f67d6
2f80f51188dc9aea697868864d88925d64c26abc	2017-01-28 11:33:43	Vicious Panda (Checkpoint)

SHA	Timestamp	Description
302cf1a90507efbded6b8f53e380591a3eaf6dcb	2019-04-25 01:15:40	Mikroceen 32-bit
21ffd24b8074d7cffdf4cc339d1fa8fe892eba27	2018-12-10 07:46:25	Mikroceen 64-bit
5192023133dce042da8b6220e4e7e2e0dcb000b3	2019-03-11 12:14:09	Mimikatz
c18602552352fee592972603262fe15c2cdb215a	2015-03-16 03:29:39	Lateral Movement via WMI
4de4b662055d3083a1bccf2bc49976cdd819bc01	2015-12-31 03:10:15	Gh0st RAT

References

- Vasily Berdnikov, Dmitry Karasovsky, Alexey Shulmin: “Microcin malware”, Kaspersky Labs 2017-9-25
- Josh Grunzweig, Robert Falcone: “Threat Actors Target Government of Belarus Using CMSTAR Trojan”, September 2017
- Checkpoint Research: “Vicious Panda: The COVID Campaign”, 2020-03-12
- SecDev Group & Citizenlab, “Tracking GhostNet: Investigating a Cyber Espionage Network”, March 2009,
- Dhia Mahjoub, Jeremiah O’Connor, Thibault Reuille, Thomas Mathew: “Phishing, Spiking, and Bad Hosting”, Cisco Umbrella Blog, 2015-09-14
- “Mimikatz: A little tool to play with Windows security”
- Peter Kálnai, Anton Cherepanov. “Lazarus KillDisks Central American casino”, WeLiveSecurity.com, April 2018
- Anton Cherepanov, Robert Lipovský: “New TeleBots backdoor: First evidence linking Industroyer to NotPetya”, WeLiveSecurity.com, October 2018
- Zuzana Hromcová: “Okrum: Ke3chang group targets diplomatic missions”, WeLiveSecurity.com, July 2019
- Avast Threat Intelligence, GitHub repository
- ESET Threat Intelligence, GitHub repository

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Execution	T1035	Service Execution	The RAT is configured to run as a service at startup via sc.exe.
T1059	Command-Line Interface	The RAT can execute a command line.	
T1064	Scripting	The attackers used batch scripts for malware installation and execution.	
T1105	Remote File Copy	The RAT can download files to the victim’s machine	
T1106	Execution through API	The RAT launches the Windows console via CreateProcess.	
Persistence	T1050	New Service	The RAT is executed automatically
Defense Evasion	T1036	Masquerading	The RAT disguises itself as various types of legitimate services.
T1140	Deobfuscate/Decode Files or Information	The commands of the RAT and some of its components are encoded/encrypted.	
Discovery	T1082	System Information Discovery	The RAT sends information, like the version of the operating system to be displayed, in operator’s panel.
T1016	System Network Configuration Discovery	The RAT collects network information, including host IP address and proxy information.	
T1033	System Owner/User Discovery	The RAT sends information, like the username to be displayed, in operator’s panel.	
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	Mimikatz is used in the attack.

Tactic	ID	Name	Description
Command and Control	T1032	Standard Cryptographic Protocol	The RAT uses SSL for encrypting C2 communications.
T1043	Commonly Used Port	The RAT uses port 443.	
T1071	Standard Application Layer Protocol	The RAT uses the Schannel implementation of SSL.	
T1001	Data Obfuscation	The RAT's interface controls the client with obfuscated commands.	
T1090.002	Proxy: External Proxy	The RAT has a proxy option that masks traffic between the malware and the remote operators.	
Exfiltration	T1041	Exfiltration Over Command and Control Channel	The operator of the RAT can download any desired file from a victim.
Collection	T1113	Screen Capture	The RAT can capture the victim's screen.

14 May 2020 - 02:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion