UBoatRAT Navigates East Asia

By Kaoru Hayashi

Published: 2017-11-28 · Archived: 2026-04-06 01:10:04 UTC

Executive Summary

Palo Alto Networks Unit 42 has identified attacks with a new custom Remote Access Trojan (RAT) called UBoatRAT. The initial version of the RAT, found in May of 2017, was simple HTTP backdoor that uses a public blog service in Hong Kong and a compromised web server in Japan for command and control. The developer soon added various new features to the code and released an updated version in June. The attacks with the latest variants we found in September have following characteristics.

- Targets personnel or organizations related to South Korea or video games industry
- Distributes malware through Google Drive
- Obtains C2 address from GitHub
- Uses Microsoft Windows Background Intelligent Transfer Service(BITS) to maintain persistence.

Targets

We don't know the exact targets at the time of this writing. However, we theorize the targets are personnel or organizations related to Korea or the video games industry. One of the reasons for the hypothesis is the file names used by the attacker when delivering the malware. We see Korean-language game titles, Korea-based game company names and some words used in the video games business on the list. Another reason is that UBoatRAT performs malicious activities on the compromised machine only when joining an Active Directory Domain. Most home user systems are not part of a domain, and as such would not be impacted the same way. Below are some of the file names associated with UBoatRAT deliveries. The first three file names are written in Korean and only includes the general business topics. Last one contains unreleased game title, “Project W’ and the Korean-based video game company’s name.

- 2017년 연봉인상 문의 사항관련 피드백 조사.exe (2017 annual salary raise inquiry related feedback survey)
- 2017년 연봉인상 문의 사항관련 피드백 전달.exe (2017 annual salary raise feedback)
- [사업]roykim's_**resume**exe ([Business]RyoKim's__resume__20170629.exe)
- [Project W]Gravity business cooperation.exe

Delivery and Installation

We observed multiple variants of UBoatRAT delivered from Google Drive. Not all of the links were active at the time of our analysis, but some (including the one below) were.

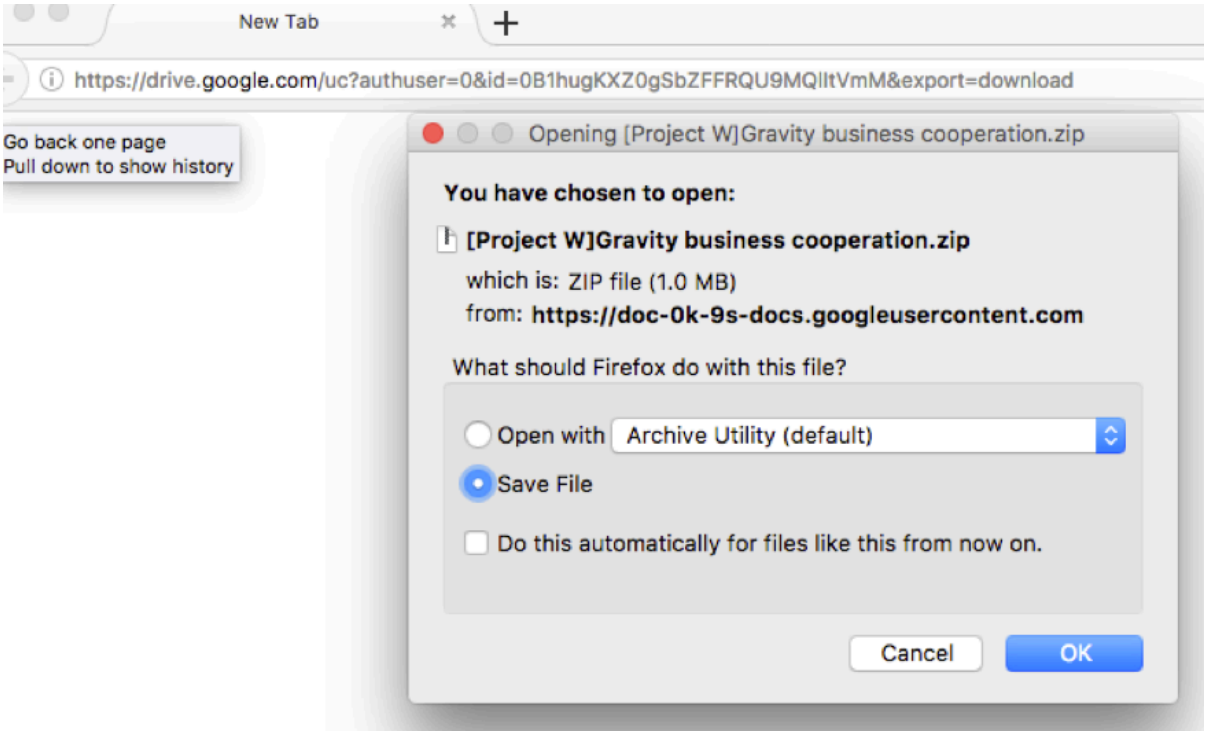

Figure 1 Download from Google Drive

The zip archive hosted on Google Drive contains the malicious executable file disguised as a folder or a Microsoft Excel spread sheet. The latest variants of the UBoatRAT released in late July or later masquerade as Microsoft Word document files.

Figure 2 Examples of UBoatRAT Masquerading

When executed, the UBoatRAT checks for the following two conditions on the compromised machine.

- Detecting virtualization software such as VMWare, VirtualBox or QEmu.
- Obtaining Domain Name from network parameters

If the RAT detects virtual environment or fails to get the domain name, it displays following fake error message and quits.

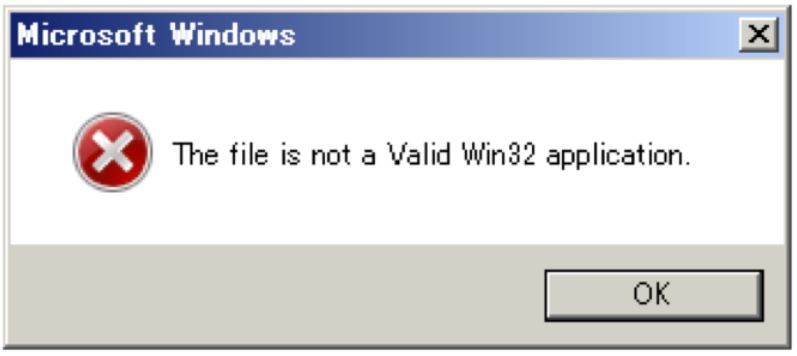

Figure 3 Fake error message

Otherwise, UBoatRAT copies itself as C:\programdata\svchost.exe, creates C:\programdata\init.bat and executes the bat file. Then displays the following message and quits.

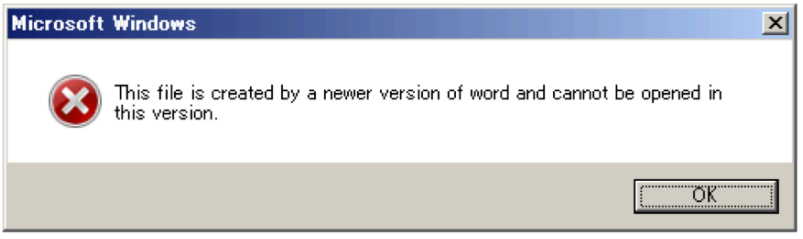

Figure 4 Fake Error Message after installation

Persistence with BITS

UBoatRAT achieves persistence by using Microsoft Windows Background Intelligent Transfer Service(BITS). BITS is a service for transferring files between machines. Though the most famous application using the service is Windows Update, other applications or users can take advantage of the component. Bitsadmin.exe is a command-line tool user can create and monitor BITS jobs. The tool provides the option, /SetNotifyCmdLine which executes a program when the job finishes transferring data or is in error. UBoatRAT takes advantage of the option to ensure it stays running on a system, even after a reboot.

The following is the contents of the init.bat. At the second line, the local file net.exe is specified to transfer to %temp%.log. After completing the copying the local file, BITS executes the UBoatRAT file configured with /SetNotifyCmdLine at the third line.

```
bitsadmin /create d1f2g34
bitsadmin /addfile d1f2g34 c:\windows\system32\net.exe  %temp%\sys.log
bitsadmin /SetNotifyCmdLine d1f2g34 "c:\programdata\svchost.exe" ""
bitsadmin /Resume d1f2g34
Del %0
```

The BITS job keeps executing the malware periodically even if the computer reboots. To remove the job from the queue, BITS needs to call Complete or Cancel explicitly. According to the article from Microsoft, the job remains 90 days by default if you don't call Complete or Cancel.

C2 communication and backdoor commands

The attacker behind the UBoatRAT hides the C2 address and the destination port in a file hosted on Github, using a URL like the following:

https://raw.githubusercontent[.]com/r1ng/news/master/README.md
The malware accesses the URL and decodes the characters between the string “[Rudeltaktik]” and character “!” using BASE64. "Rudeltaktik" is the German military term which describes the strategy of the submarine warfare during the World War II.
In the case below, the string can be decoded to 115.68.49[.]179:80.
[Rudeltaktik]MTE1LjY4LjQ5LjE3OTo4MA==!
UBoatRAT uses a custom command and control protocol to communicate with the attacker’s server. The malware places the string '488' (0x34, 0x38, 0x38 in HEX) at the top of the payload or instruction and encrypts the entire buffer with the static key 0x88 by using simple XOR cipher. Then the network payload always starts with 0xBC, 0xB0, 0xB0.

Figure 5 '488' marker

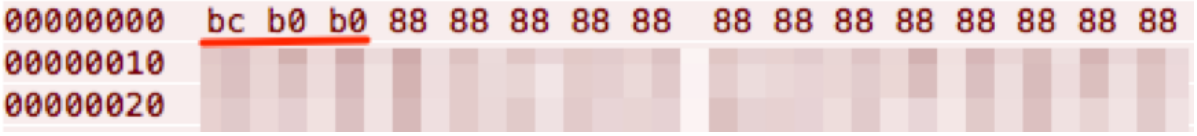

Figure 6 Encrypted '488' marker by static key

We assume the attacker picks '488' from [one of the German submarines] because the author calls the RAT UBoat-Server.

```
.vmp1:000007FEEB1C6C76                                          ; "h
.vmp1:000007FEEB1C6C7A aHjk            db 'hjk',0               ; DA
.vmp1:000007FEEB1C6C7E aUboatServerDll db 'UBoat_Server_DLL.dll',0
```

Figure 7 UBoat_Server in the malware

After establishing a covert channel with C2, the threat waits following backdoor commands from the attacker.

Command	Description
alive	Checks if whether the RAT is alive
online	Keeps the RAT online by sending the packets to C2 periodically
upfile	Uploads file to compromised machine
downfile	Downloads file from compromised machine
exec	Executes process with [UAC Bypass using Eventvwr.exe and Registry Hijacking]
start	Starts CMD shell
curl	Downloads file from specified URL

pslist	Lists running processes
pskill	Terminates specified process

Development of UBoatRAT

At the time of this writing, we have identified fourteen samples of UBoatRAT and one downloader associated with the attacks. Most of UBoatRAT samples retrieve C2 address from GitHub as described above. Only one sample released in May connected to public blog service in Hong Kong and compromised legitimate web server in Japan as C2. The sample uses regular HTTP protocol for communication. The account for the blog, 'elsa_kr' has existed since April 2016 and has no meaningful contents at this moment.

Figure 8 Public Blog used as C2

The author released a new version employing various new features in June. The early version of this new version obtains a C2 address from the repository 'uuu' owned by the GitHub account 'elsa999'. At the time of this writing, the 'uuu' repository has been deleted. It has since been replaced by three other repositories ('uj', 'hhh' and 'enm') all hosting an encoded combination of IP address and port in the account. According to the file history, the author has frequently been updating these files since July. After performing a quick analysis, we concluded these three repositories are for development and testing purpose for following reasons.

- They use the different marker '###NEWS###', instead of '[Rudeltaktik]'.
- The encoded global IP addresses are different from known UBoatRAT samples.
- The author always changes the encoded address back to localhost(127.0.0.1) in short period.

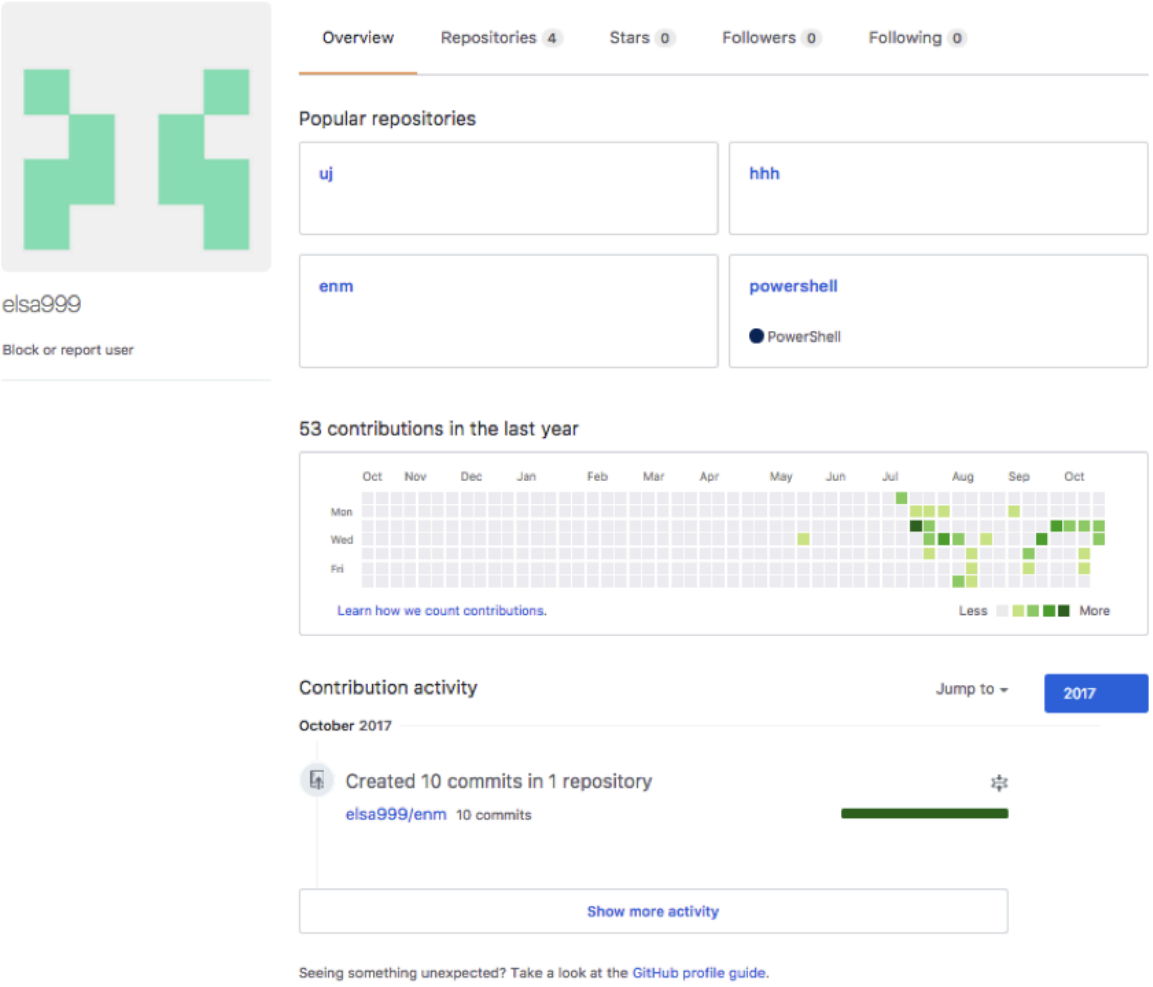

Figure 9 GitHub account for testing

The 'elsa999' user also has the following three PowerShell scripts in their repositories. These scripts are written by other authors for penetration testing.

- gpp_autologon.ps1
- gpp_pwd.ps1
- wmi_scan.ps1

Conclusion

Though the latest version of UBoatRAT was released in September, we have seen multiple updates in elsa999 accounts on GitHub in October. The author seems to be vigorously developing or testing the threat. We will continue to monitor this activity for updates.

Palo Alto Networks customers are protected from this threat in the following ways:

- All samples discussed are classified as malicious by the WildFire and Threat Prevention
- Traps prevents the malware discussed in this report from executing
- AutoFocus users can track the malware described in this report using the UBoatRAT

Indicators

UBoatRAT SHA256

bf7c6e911f14a1f8679c9b0c2b183d74d5accd559e17297adcd173d76755e271
6bea49e4260f083ed6b73e100550ecd22300806071f4a6326e0544272a84526c
cf832f32b8d27cf9911031910621c21bd3c20e71cc062716923304dacf4dadb7
7b32f401e2ad577e8398b2975ecb5c5ce68c5b07717b1e0d762f90a6fbd8add1
04873dbd63279228a0a4bb1184933b64adb880e874bd3d14078161d06e232c9b
42d8a84cd49ff3afacf3d549fbab1fa80d5eda0c8625938b6d32e18004b0edac
7be6eaa3f9eb288de5606d02bc79e6c8e7fc63935894cd793bc1fab08c7f86c7
460328fe57110fc01837d80c0519fb99ea4a35ea5b890785d1e88c91bea9ade5
55dd22448e9340d13b439272a177565ace9f5cf69586f8be0443b6f9c81aa6e7
9db387138a1fdfa04127a4841cf024192e41e47491388e133c00325122b3ea82
e52d866e5b77e885e36398249f242f8ff1a224ecce065892dc200c57595bb494
eb92456bf3ab86bd71d74942bb955062550fa10248d67faeeeedd9ff4785f41e
452b1675437ef943988c48932787e2e4decfe8e4c3bed728f490d55b3d496875
66c2baa370125448ddf3053d59085b3d6ab78659efee9f152b310e61d2e7edb5

Downloader SHA256

f4c659238ffab95e87894d2c556f887774dce2431e8cb87f881df4e4d26253a3

Web Access

https://raw.githubusercontent[.]com/r1ng/news/master/README.md
https://raw.githubusercontent[.]com/elsa999/uuu/master/README.md
http://www.ak(masked)[.]jp/images/ http://elsakrblog.blogspot[.]hk/2017/03/test.html

C2

115.68.49[.]179:80
115.68.49[.]179:443
60.248.190[.]36:443
115.68.52[.]66:443
115.68.49[.]180:443
122.147.187[.]173:443
124.150.140[.]131:443

File

C:\programdata\init.bat
C:\programdata\svchost.exe

Source: https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/