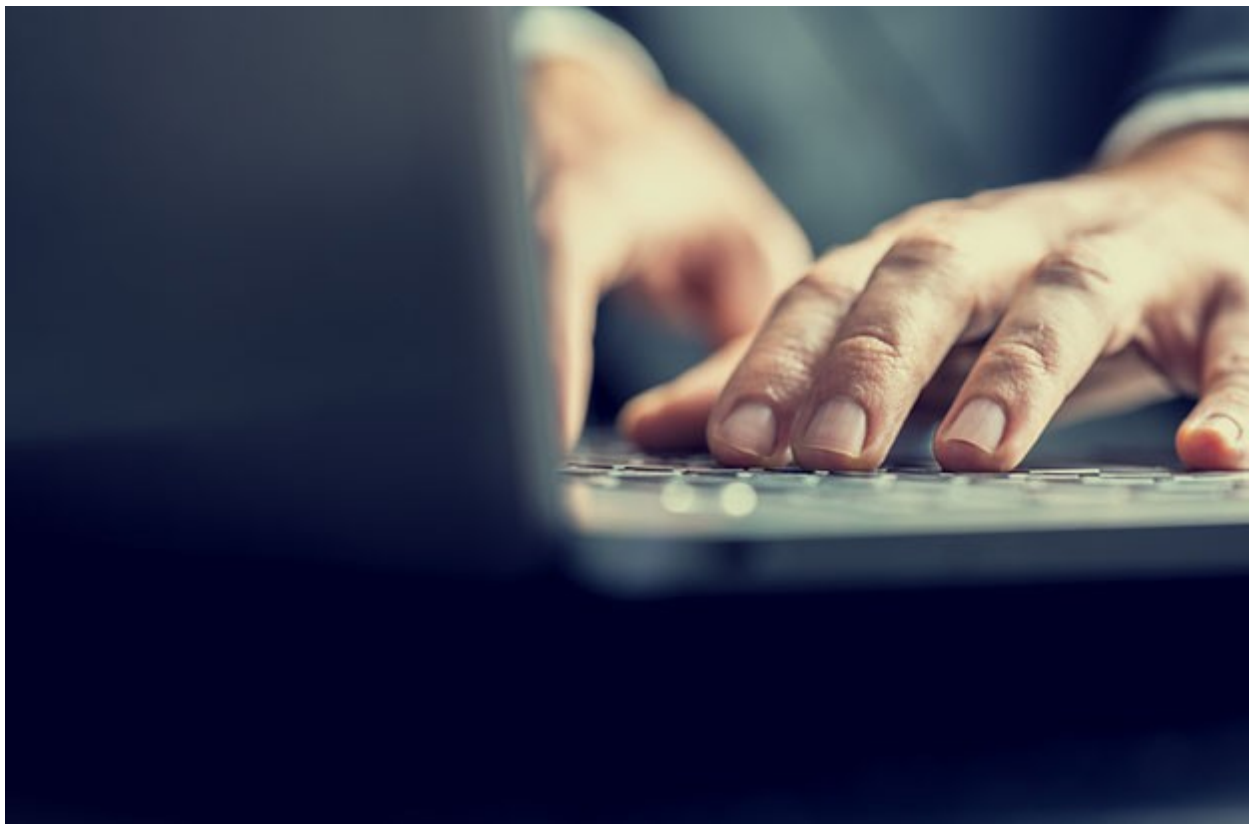
Korplug military targeted attacks: Afghanistan & Tajikistan

welivesecurity.com/2014/11/12/korplug-military-targeted-attacks-afghanistan-tajikistan/

November 12, 2014



After taking a look at recent Korplug (PlugX) detections, we identified two larger scale campaigns employing this well-known Remote Access Trojan. This blog gives an overview of the first one

12 Nov 2014 - 03:17PM

After taking a look at recent Korplug (PlugX) detections, we identified two larger scale campaigns employing this well-known Remote Access Trojan. This blog gives an overview of the first one

After taking a look at recent Korplug (PlugX) detections, we identified two larger scale campaigns employing this well-known Remote Access Trojan. This blog gives an overview of the first one, related to Afghanistan & Tajikistan. The other campaign, where the targets were a number of high-profile organizations in Russia, will be the subject of **Anton Cherepanov's presentation at the ZeroNights security conference in Moscow this week.**

Sometimes malware used in various attacks is unique enough to identify related incidents, which makes tracking individual botnets simpler. An example is the BlackEnergy Lite variant (also known as BlackEnergy 3) used by a group of attackers (that was then given the name Quedagh, or Sandworm) against targets in Ukraine and other countries. BlackEnergy Lite is clearly distinguishable from the numerous binaries of the more common BlackEnergy 2 also circulating in-the-wild.

In other cases, attackers use more common tools for accomplishing their criminal goals. For example, the Korplug RAT (a.k.a .PlugX) is a well-known toolkit associated with Chinese APT groups and used in a large number of targeted attacks since 2012. For the past several weeks we have taken a closer look at a great number of detections of this malware in many unrelated incidents.

Among these, we were able to discover several successful infections where the employed Korplug samples were connecting to the same C&C domain.

DOMAIN: www.notebookhk.net
Updated Date: 2013-11-12 18:03:45
Create Date: 2013-06-18 11:08:17
Registrant Name: lee stan
Registrant Organization: lee stan
Registrant Street: xianggangdiqu
Registrant City: xianggangdiqu
Registrant State: xianggang
Registrant Postal Code: 796373
Registrant Country: HK
Registrant Phone : +0.04375094543
Registrant Fax: +0.04375094543
Registrant Email:stanlee@gmail.com

Other Korplug samples were connecting to a different domain name resolving to the same IPs as notebookhk.net:

DOMAIN: www.dicemention.com
Updated Date: 2013-11-12 18:05:33
Create Date: 2013-09-10 14:35:11
Registrant Name: z x
Registrant Organization: z x
Registrant Street: xianggangdiqu
Registrant City: xianggangdiqu
Registrant State: xianggang
Registrant Postal Code: 123456
Registrant Country: HK

Registrant Phone : +0.0126324313
Registrant Fax: +0.0126324313
Registrant Email: 123@123.com

DOMAIN: www.abudlrasul.com
Updated Date: 2014-10-16 14:16:27
Create Date: 2014-10-16 14:16:27
Registrant Name: gang xin
Registrant Organization: gang xin
Registrant Street: Argentina Argentina
Registrant City: Argentina
Registrant State: Argentina
Registrant Postal Code: 647902
Registrant Country: AR
Registrant Phone : +54.0899567089
Registrant Fax: +54.0899567089
Registrant Email: woffg89@yahoo.com

Taking these C&Cs as a starting point, we were able to locate a number of victims infected through various exploit-laden spear-phishing documents and cunningly-named archives.

A table with a selection of RTF documents and RAR self-extracting archives with a .SCR extension is shown below:

File name	English translation	SHA1
Situation Report about Afghan.doc		36119221826D0290BC23371B55A8C0E6A84718DD
AGREEMENT BETWEENTHE NATO AND AFGHANISTAN ON THE STATUS OF NATO FORCES IN AFGHANISTAN.doc		A6642BC9F3425F0AB93D462002456BE231BB5646
news.doc		51CDC273B5638E06906BCB700335E288807744B5
План деятельности соединений и воинских частей Приволжского региона на июль 2014 г.scr	Activity plan for military units in the Volga region in July 2014	EA6EE9EAB546FB9F93B75DCB650AF22A95486391

File name	English translation	SHA1
телефонный справочник структуры МИД КР .scr	Telephone directory of the Ministry of Foreign Affairs of the Kyrgyz Republic	D297DC7D29E42E8D37C951B0B11629051EEBE9C0
О Центре социальной адаптации военнослужащих.scr	About the Center for social adaptation of servicemen	8E5E19EBE719EBF7F8BE4290931FFA173E658CB8
Протокол встречи НГШ КНР.scr	Meeting minutes of the General Staff of the PRC	1F726E94B90034E7ABD148FE31EBA08774D1506F
исправленный шаблон плана мероприятий.scr	Corrected action plan template	A9C627AA09B8CC50A83FF2728A3978492AEB79D8
Situation Report about Afghan.scr		A9C627AA09B8CC50A83FF2728A3978492AEB79D8
Военно-политическая обстановка в ИРА на04.10.2014.scr	Military and political situation in Islamic Republic of Afghanistan (IRA) on 04.10.2014	E32081C56F39EA14DFD1E449C28219D264D80B2F
Afghan Air Force.scr		E32081C56F39EA14DFD1E449C28219D264D80B2F
план мероприятий.scr	Action plan	1F726E94B90034E7ABD148FE31EBA08774D1506F

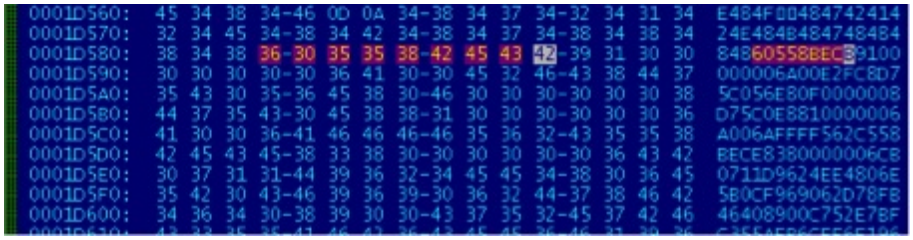
Some of the above-mentioned files also contained decoy documents:

In all of the cases, three binary files were dropped (apart from decoy documents) that led to the Korplug trojan being loading into memory.

- exe – a legitimate executable with a Kaspersky digital signature that would load a DLL with a specific file name
- dll – a small DLL loader that would pass execution to the Korplug raw binary code
- dll.avp – raw Korplug binary

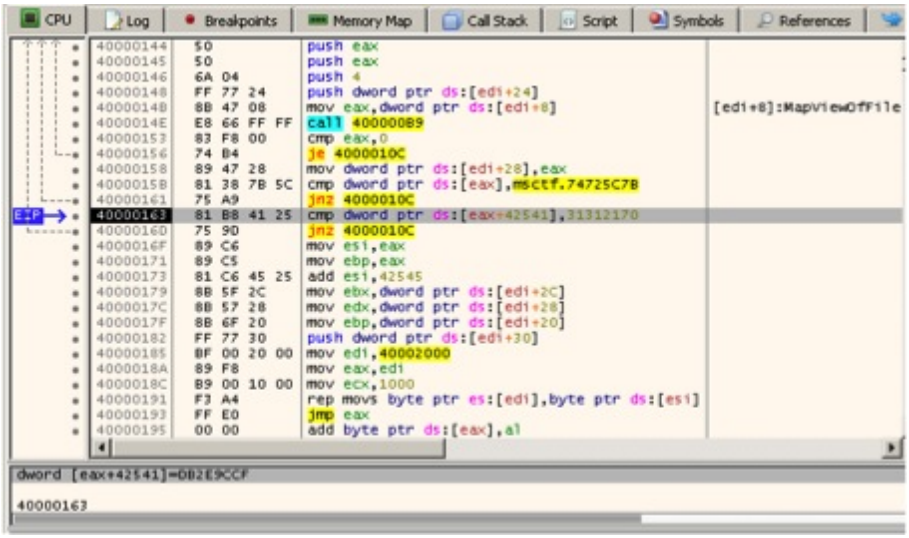
The Korplug RAT is known to use this side-loading trick by abusing legitimate digitally signed executables and is a way to stay under the radar, since a trusted application with a valid signature among startup items is less likely to raise suspicion.

The maliciously crafted documents are RTF files that successfully exploit the CVE-2012-0158 vulnerability in Microsoft Word. The image below shows the beginning of the CVE-2012-0158 shellcode in ASCII encoding within the document (the opcodes 60, 55, 8bec disassemble to pusha; push ebp; mov ebp, esp).



Interestingly, though, the documents also contain the newer CVE-2014-1761 exploit that was extensively used in targeted attacks carried out by a number other malware families this year (including BlackEnergy, Sednit, MiniDuke, and others). However, this exploit is not implemented correctly due to a wrong file offset in the 1st stage shellcode.

Below we see the disassembly of the 1st stage shellcode where it checks the presence of the tag “p!11” marking the beginning of the 2nd stage shellcode and loads it into memory. Even though the tag and 2nd stage shellcode is present in the RTF, it’s at a different offset, and thus never is loaded.



Sophos’ Gabor Szappanos gives a possible explanation how these malformed samples may have come into existence.

ESET LiveGrid telemetry indicates that the attacks against these targets have been going on since at least June 2014 and continue through today.

We were able to pinpoint the targets to residents of the following countries:

- Afghanistan

- Tajikistan
- Russia
- Kyrgyzstan
- Kazakhstan

From the topics of the files used to spread the malware, as well as from the affected targets, it appears that the attackers are interested in gathering intelligence related to Afghan, Tajik and Russian military and diplomatic subjects.

Interestingly, most of the affected victims have another thing in common – a number of other RATs, file stealing trojans or keyloggers were detected on their systems on top of the Korplug RAT detection. One of these 'alternative RATs' was connecting to a domain also used by the Korplug samples.

Since the functionality of these tools was partly overlapping with that of Korplug, it left us wondering whether the attackers were just experimenting with different RATs or were they supplementing some functionality that they were unable to accomplish.

Additional information about two malware families that were most often found accompanying Korplug infections is given below.

Alternative Malware #1: DarkStRat

A curious Remote Access Trojan, as research points to a Chinese connection but the commands it listens to are in Spanish (translation in English):

- CERRAR (close)
- DESINSTALAR (uninstall)
- SERVIDOR (server)
- INFO
- MAININFO
- PING
- REBOOT
- POWEROFF
- PROC
- KILLPROC
- VERUNIDADES (see units)
- LISTARARCHIVOS (list files)
- EXEC
- DELFILE
- DELFOLDER
- RENAME
- MKDIR
- CAMBIOID (change ID)

- GETFILE/SENDFILE/RESUMETRANSFER
- SHELL
- SERVICIOSLISTAR (list service)
- INICIARSERVICIO (start service)
- DETENERSERVICIO (stop service)
- BORRARSERVICIO (erase service)
- INSTALARSERVICIO (install service)

The malware can manage processes and services on the infected machine, transfer files to and from the C&C server, run shell commands, and so on. It is written in Delphi and connects to www.dicemention.com. Some samples contain a digital signature by “Nanning weiwu Technology co.,ltd”.

Alternative Malware #2: File Stealer

This malware, written in C, and contains several functions for harvesting files off the victim’s hard drive according to criteria set in the configuration file. Apart from doing a recursive sweep of all logical fixed and remote drives, it also continually monitors any attached removable media or network shares by listening to DBT_DEVICEARRIVAL events.

In addition to collecting files, the malware attempts to gather saved passwords, history of visited URLs, account information and proxy information from the following applications:

- Microsoft Messenger
- Microsoft Outlook
- Microsoft Internet Explorer
- Mozilla Firefox

The C&C domains used by this malware are:

- newvinta.com
- worksware.net

Some samples of this file stealer detected in these campaigns also contain the signature by “Nanning weiwu Technology co.,ltd” – another indicator that the infections are related.

List of SHA1 hashes:

Korplug:

5DFA79EB89B3A8DDBC55252BD330D04D285F9189
095550E3F0E5D24A59ADD9390E6E17120039355E
5D760403108BDCDCE5C22403387E89EDC2694860
05BFE122F207DF7806EB5E4CE69D3AEC26D74190
548577598A670FFD7770F01B8C8EEFF853C222C7

530D26A9BEEDCCED0C36C54C1BF3CDA28D2B6E62
F6CB6DB20AA8F17769095042790AEB60EECD58B0
EF17B7EC3111949CBDBDEB5E0E15BD2C6E90358F
17CA3BBDDEF164E6493F32C952002E34C55A74F2
973EA910EA3734E45FDE304F20AB6CF067456551
47D78FBFB2EFC3AB9DDC653A0F03D560D972BF67
0B5A7E49987EF2C320864CF205B7048F7032300D
E81E0F416752B336396294D24E639AE86D9C6BAA
E930D3A2E6B2FFDC7052D7E18F51BD5A765BDB90

Alternative Malware #1:

FDD41EB3CBB631F38AC415347E25926E3E3F09B6
457F4FFA2FE1CACFEA53F8F5FF72C3FA61939CCD
5B6D654EB16FC84A212ACF7D5A05A8E8A642CE20
7D59B19BD56E1D2C742C39A2ABA9AC34F6BC58D4
D7D130B8CC9BEA51143F28820F08068521763494
01B4B92D5839ECF3130F5C69652295FE4F2DA0C5
02C38EC1C67098E1F6854D1125D3AED6268540DE

Alternative Malware #2:

3A7FB6E819EEC52111693219E604239BD25629E9
BF77D0BA7F3E60B45BD0801979B12BEA703B227B
55EF67AFA2EC2F260B046A901868C48A76BC7B72
A29F64CD7B78E51D0C9FDFBDCBC57CED43A157B2
34754E8B410C9480E1ADFB31A4AA72419056B622
17A2F18C9CCAAA714FD31BE2DE0BC62B2C310D8F
6D99ACEA8323B8797560F7284607DB08ECA616D8
1884A05409C7EF877E0E1AAAEC6BB9D59E065D7C
1FC6FB0D35DCD0517C82ADAEF1A85FFE2AFAB4EE
5860C99E5065A414C91F51B9E8B779D10F40ADC4
7950D5B57FA651CA6FA9180E39B6E8CC1E65B746

Research by: Anton Cherepanov

12 Nov 2014 - 03:17PM

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

---

Newsletter

Discussion