Innaput Actors Utilize Remote Access Trojan Since 2016, Presumably Targeting Victim Files

asert.arbornetworks.com/innaput-actors-utilize-remote-access-trojan-since-2016-presumably-targeting-victim-files/

NETSCOUT Blog

by ASERT Team on April 4th, 2018

Overview

ASERT recently identified a campaign targeting commercial manufacturing in the US and potentially Europe in late 2017. The threat actors used phishing and downloader(s) to install a Remote Access Trojan (RAT) ASERT calls InnaputRAT on the target's machine. The RAT contained a series of commands that includes machine profiling and the ability to exfiltrate documents from the victims' machines. We believe this activity ties to a specific set of actors with defined campaign goals. We've also observed similarities in binaries dating back to 2016, a clear indication that these threat actors have operated for nearly two years.

Key Findings

- InnaputRAT, a RAT capable of exfiltrating files from victim machines, was distributed by threat actors using phishing and Godzilla Loader.
- The RAT has evolved through multiple variants dating back to 2016.
- Recent campaigns distributing InnaputRAT beaconed to live C2 as of March 26, 2018.

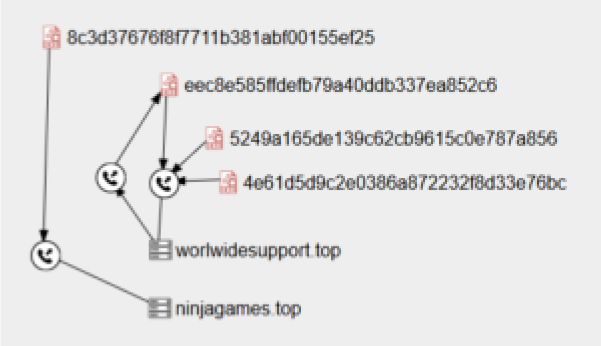

8c3d37676f8f7711b381abf00155ef25
eec8e585ffdefb79a40ddb337ea852c6
5249a165de139c62cb9615c0e787a856
4e61d5d9c2e0386a872232f8d33e76bc
worlwidesupport.top
ninjagames.top

Figure 1: InnaputRAT communicating to TOP domains.

Attribution

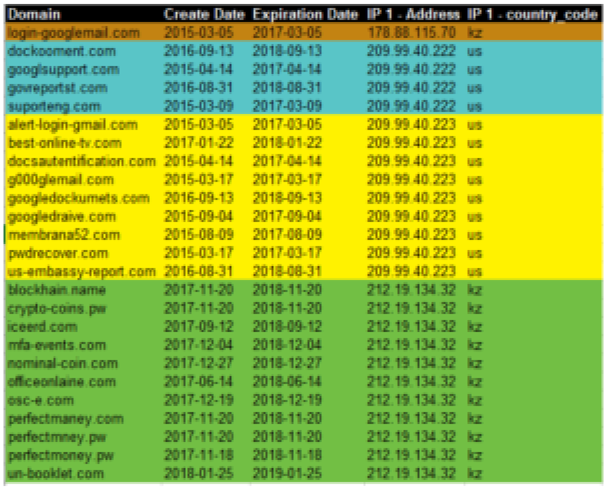
ASERT identified potential actors, or personas, tied to this campaign through domains registrations, Facebook, and Twitter accounts possibly tied to an email address used. We initially identified the campaign through several phishing attempts that led to additional infrastructure within the same campaign. This campaign shared a common malware payload, InnaputRAT. Some of the recent malware samples were attributed to the campaign through similarities in the binary rather than connected infrastructure. The phishing emails appear to lure victims with a geopolitical-theme. Sender email addresses and subject lines often reference the United Nations (UN). Further, while most of the domains associated with Aigul(Aygul) Akulova and Slabodan Miloshevich attempt to mimic Google or Microsoft products, a few of them were more specific in mimicking diplomacy related targets, notably un-booklet[.]com and us-embassy-report[.]com, suggesting a more specific audience. We identified the initial campaign through domains highlighted in the Phishing Domains section below. After analysis of the original infrastructure, we identified the InnaputRAT payload on additional infrastructure highlighted in the Additional Domains Section.

Phishing Domains

1. mfa-events[.]com
2. officeonlaine[.]com
3. blockhain[.]name
4. iceerd[.]com

All of these domains are tied to the email address s.miloshevich[@]yandex.ru with the registration name Slabodan Miloshevich. Each of the domains used Kazakhstan as the registrant's country. Additional domains registered by the same entity resolved to 4 distinct

IP addresses (as of March 24. 2017).



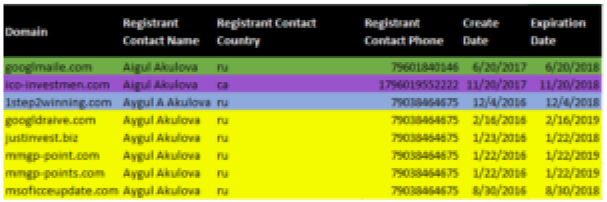
Domain	Create Date	Expiration Date	IP 1 - Address	IP 1 - country_code
login-googlemail.com	2015-03-05	2017-03-05	178.88.115.70	kz
dockooment.com	2016-09-13	2018-09-13	209.99.40.222	us
googlsupport.com	2015-04-14	2017-04-14	209.99.40.222	us
govreportst.com	2016-08-31	2018-08-31	209.99.40.222	us
suporteng.com	2015-03-09	2017-03-09	209.99.40.222	us
alert-login-gmail.com	2015-03-05	2017-03-05	209.99.40.223	us
best-online-tv.com	2017-01-22	2018-01-22	209.99.40.223	us
docsautentification.com	2015-04-14	2017-04-14	209.99.40.223	us
g000glemail.com	2015-03-17	2017-03-17	209.99.40.223	us
googledockumets.com	2016-09-13	2018-09-13	209.99.40.223	us
googledraive.com	2015-09-04	2017-09-04	209.99.40.223	us
membrana52.com	2015-08-09	2017-08-09	209.99.40.223	us
pwdrecover.com	2015-03-17	2017-03-17	209.99.40.223	us
us-embassy-report.com	2016-08-31	2018-08-31	209.99.40.223	us
blockhain.name	2017-11-20	2018-11-20	212.19.134.32	kz
crypto-coins.pw	2017-11-20	2018-11-20	212.19.134.32	kz
iceerd.com	2017-09-12	2018-09-12	212.19.134.32	kz
mfa-events.com	2017-12-04	2018-12-04	212.19.134.32	kz
nominal-coin.com	2017-12-27	2018-12-27	212.19.134.32	kz
officeonlaine.com	2017-06-14	2018-06-14	212.19.134.32	kz
osc-e.com	2017-12-19	2018-12-19	212.19.134.32	kz
perfectmaney.com	2017-11-20	2018-11-20	212.19.134.32	kz
perfectmney.pw	2017-11-20	2018-11-20	212.19.134.32	kz
perfectmoney.pw	2017-11-18	2018-11-18	212.19.134.32	kz
un-booklet.com	2018-01-25	2019-01-25	212.19.134.32	kz

Figure 2: Domains registered by s.miloshevich[@]yandex.ru

Additional Domain Analysis

1. mfa-events[.]top
2. officemicroupdate[.]com
3. ico-investmen[.]com

In the prior section we associated the first domain with s.miloshevich[@]yandex.ru. The actor behind innaput69[@]gmail.com registered domains two and three. All three domains hosted either a variant or the primary sample we analyzed, thus tying them together as part of the same activity. Looking at the domains registered by innaput69[@]gmail.com, the names on the account use the same last name but use two different first names. Notice all but one list the registrant contact country as RU.



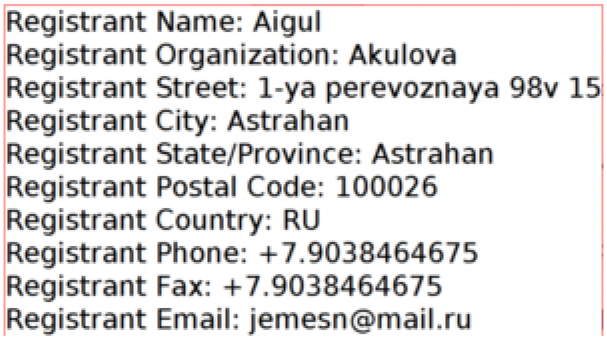
Domain	Registrant Contact Name	Registrant Contact Country	Registrant Contact Phone	Create Date	Expiration Date
googlmaile.com	Aigul Akulova	ru	79601840146	6/20/2017	6/20/2018
ico-investmen.com	Aigul Akulova	ca	1796019552222	11/20/2017	11/20/2018
1step2winning.com	Aygul A Akulova	ru	79038464675	12/4/2016	12/4/2018
googldraive.com	Aygul Akulova	ru	79038464675	2/16/2016	2/16/2019
justinvest.biz	Aygul Akulova	ru	79038464675	1/23/2016	1/22/2018
mmgp-point.com	Aygul Akulova	ru	79038464675	1/22/2016	1/22/2019
mmgp-points.com	Aygul Akulova	ru	79038464675	1/22/2016	1/22/2019
msoficceupdate.com	Aygul Akulova	ru	79038464675	8/30/2016	8/30/2018

Figure 3: Domains tied to innaput69@gmail[.]com

To find officemicroupdate[.]com we must dig through some historical domain registrar information. From March 1, 2017 – November 2, 2017 the registrant email was innaput69[@]gmail.com (according to Domain Tools) before the URL was taken over by Microsoft. Prior to March 1st of 2017 the registrant info was hidden behind a Privacy Protected Record so it is possible it was registered at one time by someone other than the actor behind innaput69[@]gmail.com.

GodZilla Loader Link

Pivoting off of the phone number for "Aygul A Akulova" in figure 3 we find another email address, jemesn[@]mail.ru. This email address is tied to a couple of other domains as well.



```
Registrant Name: Aigul
Registrant Organization: Akulova
Registrant Street: 1-ya perevoznaya 98v 15
Registrant City: Astrahan
Registrant State/Province: Astrahan
Registrant Postal Code: 100026
Registrant Country: RU
Registrant Phone: +7.9038464675
Registrant Fax: +7.9038464675
Registrant Email: jemesn@mail.ru
```

Figure 4: Registrant info for jemesn[@]mail.ru

One of the domains associated with jemesn[@]mail.ru, update-app[.]top, hosted a copy of Godzilla Loader which we observed distributing InnaputRAT late March 2018.

InnaputRAT Evolution

All of the infrastructure and registrants were tied together with a common malware payload, InnaputRAT. We identified a recent version of the InnaputRAT through the initial phishing campaigns, infastructure correlation, and binary analysis. We then found several variations of the malware dating back to 2016. The binaries are listed below in chronological order. Our starting sample (5249a165de139c62cb9615c0e787a856) is listed as Sample 3 (below). We compared the binaries using Diaphora, an open source tool for comparing programs in a decompiler, and extracted relevant information showing the RAT's evolution.

Sample 1 - May, 29 2016

MD5	2939d7350f611263596bdc0917296aa3
Compile date	2016-05-29 13:38:07
PDB	N/A
ITW	N/A
C2s:	officemicroupdate[.]com
Communication Port:	5876
File Name:	msupdate.exe
Persistence:	Maldoc (27dac1fa017006933eaf2b044df0b443) drops a Dropper that creates a Windows Service (OfficeUpdateService) and executes the payload

Command Options	Function Name: sub_401737 1. GetDriveAndVolInfo 2. GetFileAttributeW 3. EnumDirectory 4. ReadFile (CreateFileMapping -> MapViewOfFile) 5. WriteFile 6. DeleteFile 7. ShellExecuteW 8. GetSystemInfo
Diaphora Function Match Stats	Matches: 14 Unmatched: 30 - Includes sub_401737
Notes:	• Dropped via: 27dac1fa017006933eaf2b044df0b443 • Linked to officemicroupdate[.]com via 185[.]61[.]151[.]110

Table 1: Sample 1 Analysis

We believe this to be an earlier variant of for the following reasons:

- The “Command Options” used reflect later variants. The order of the options also reflects other variants.
- Although it doesn’t share as many matching functions as other samples, some of the binary structure matched newer variants.

While we believe this sample is from the same family as Samples 2 through 5 (below), there are some notable differences that suggest the malware evolved over time:

- Persistence method
    - This sample makes use of a service installed by a dropper file. In contrast, other samples use the Windows registry to install an Autorun key.
    - Notably, the payload requires the dropper for execution and remains dormant if it is not present on the victim machine.
- Windows API Calls

    The *Read File* command for this sample used CreateFileMapping and MapViewOfFile while newer samples used CreateFileW and ReadFile.

The key functionality of the payload remains the same across all binaries: browse the victim file system with the intent to exfiltrate desired data.

Sample 2 - June 5, 2017

Sample 2 looks more like our starting point (Sample 3).

MD5	8c3d37676f8f7711b381abf00155ef25
Compile date	2017-06-05 16:57:38
PDB	D:\Arena\RobotNet\FileTransferStream\Release\FileTransfer.pdb
ITW	hxxp://best-online-tv[.]com/1.exe
C2s:	worlwidesupport[.]top ninjagames[.]top ajdhsfhiudsfhsi[.]top
Communication Port:	52100
File Name:	SafeApp.exe
Persistence:	HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Run: %appdata%\SafeApp\SafeApp.exe
Command Options:	Function Name: sub_401B46 1. GetDriveVolInfo 2. GetFileAttributesW 3. EnumDirectory 4. ReadFile (CreateFileW + ReadFile) 5. WriteFile 6. DeleteFile 7. ShellExecuteW 8. GetSystemInfo
Diaphora Function Match Stats	Matches: 36 - Includes sub_401B46 Unmatched: 4

Table 2: Sample 2 Analysis

Performing a diffing operation using Diaphora, most of the functions in the binary matched, including “Command Options” and C2s used. This provides an increased level of confidence that Sample 2 is a variant of the “ground zero” binary in Sample 3 (below). The key difference between later variants and Sample 1, involve the persistence mechanism used and a change in the Read File “Command Option”. Later variants no longer rely on the dropper to set persistence via Windows Service, but instead create the Windows Registry key as seen in Table 2 and execute the malware.

Sample 3 - August 22, 2017

Sample 3, our starting sample , is a near exact match with Sample 2, but seen hosted on a different server.

MD5	5249a165de139c62cb9615c0e787a856
Compile date	2017-08-22 15:58:14
PDB	N/A
ITW	hxxp://mfa-events[.]com/upd.exe
C2s:	worlwidesupport[.]top ninjagames[.]top ajdhsfhiudsfhsi[.]top
Communication Port	52100
File Name	NeutralApp.exe
Persistence	HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Run: %appdata%\NeutralApp\NeutralApp.exe
Command Options	Function Name: sub_401E39 1. GetDriveVolInfo 2. GetFileAttributesW 3. EnumDirectory 4. ReadFile (CreateFileW + ReadFile) 5. WriteFile 6. DeleteFile 7. ShellExecuteW 8. GetSystemInfo
Diaphora Function Match Stats	Not done as this is the starting sample.

Table 3: Sample 3 Analysis

The primary difference between Sample 2 and this sample is the file name used by the payload. The prior version used the name SafeApp.exe and installed the binary into %AppData% and added a Windows auto run registry entry against that file. Sample 3 does the same thing but makes the file name NeutralApp.exe. This is notable, because the malware checks for a copy of itself, and the name is static making it simple to identify infection. Due to the name change, the newer version runs even if SafeApp.exe is currently running on the victim machine.

Sample 4 - January 22, 2018

Continuing binary matching and infrastructure analysis, we found a fourth sample that showed more evolution of the binary by obfuscating some of the API names and strings. This binary also shared the same NeutralApp.exe file name and the same C2s as the prior variant. The “Command Options” also remained the same in this variant.

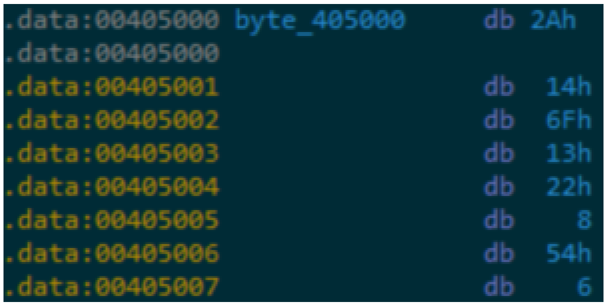
MD5	4e61d5d9c2e0386a872232f8d33e76bc
Compile date	2018-01-22 20:46:41
PDB	D:\Arena\RobotNet\FileTransferStream\Release\FileTransfer.pdb
ITW	hxxp://ico-investmen[.]com/1.exe
C2s:	worlwidesupport[.]top ninjagames[.]top ajdhsfhiudsfhsi[.]top
Communication Port:	52100
File Name:	NeutralApp.exe
Persistence:	HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Run: %appdata%\NeutralApp\NeutralApp.exe
Command Options	Function Name: sub_401F95 No change
Diaphora Function Match Stats	Matches: 33 - sub_401F95 Unmatched: 13
Notes:	Some API names and registry strings are obfuscated.

Table 4: Sample 4 Analysis

The PDB string contained in this fourth sample is identical to Sample 2, further lending credence to the evolution of the InnaputRAT.

API & String Obfuscation

This variant uses an 8-byte XOR key to obfuscate API names and other strings within the payload (Figure 5).



```
.data:00405000 byte_405000     db 2Ah
.data:00405000
.data:00405001                 db  14h
.data:00405002                 db  6Fh
.data:00405003                 db  13h
.data:00405004                 db  22h
.data:00405005                 db    8
.data:00405006                 db  54h
.data:00405007                 db    6
```

Figure 5: 8-Byte XOR Key for obfuscation

Sample 5 - March 13, 2018

The most recent variant of the InnaputRAT also shared the same C2s as the previous two samples, the same NeutralApp.exe name, and the same Registry Key creation. At the time of our analysis of this sample, the payload was being distributed by Godzilla Loader (Figure

6), a tool sold in underground forums and used in multiple campaigns to distribute malware such as Dridex, Trickbot, and Panda Banker.

MD5	eec8e585ffdefb79a40ddb337ea852c6
Compile date	2018-03-13 18:45:45
PDB	N/A
ITW	N/A
C2s:	worlwidesupport[.]top ninjagames[.]top ajdhsfhiudsfhsi[.]top
Communication Port:	52100
File Name:	NeutralApp.exe
Persistence:	HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Run: %appdata%\NeutralApp\NeutralApp.exe
Command Options	Function Name: sub_401DA0 No change
Diaphora Function Match Stats	Best Matches: 26 - sub_401DA0 Unmatched: 27
Notes:	More string and API Name obfuscation

Table 5: Sample 5 Analysis

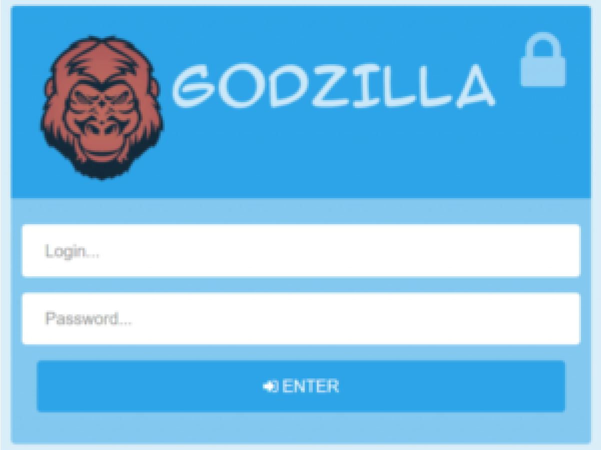
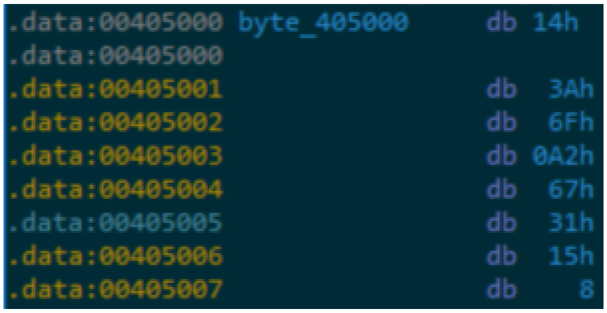


Figure 6: GodZilla Loader Login Panel

Primary differences between this sample and the previous two are diminishing matched functions using Diaphora (likely a result of the attackers obfuscating more API calls and strings) and a change in the 8-Byte XOR key used to obfuscate the API names and other strings.



```
.data:00405000 byte_405000     db 14h
.data:00405000
.data:00405001                 db  3Ah
.data:00405002                 db  6Fh
.data:00405003                 db 0A2h
.data:00405004                 db  67h
.data:00405005                 db  31h
.data:00405006                 db  15h
.data:00405007                 db    8
```

Figure 7: 8-Byte XOR key change

Summary

ASERT believes the attackers behind the InnaputRAT are primarily targeting files for exfiltration from victim machines. The initial targeting of commercial manufacturing entities possibly suggests a goal of intellectual property theft. Since 2016 the malware has undergone significant changes. The attackers continue to improve the sophistication of the bot and its operation with the inclusion of an intermediary loader, Godzilla Loader, and obfuscation of key elements in the binary. We assess with moderate confidence that this operation will continue and the InnaputRAT will continue to evolve.

Appendix A:

IOCs:

- alert-login-gmail[.]com
- blockhain[.]name
- best-online-tv[.]com
- dockooment[.]com
- docsautentification[.]com
- g000glemail[.]com
- googldraive[.]com
- googledockumets[.]com
- googledraive[.]com
- googlesuport[.]com
- googlmaile[.]com
- googlsupport[.]com
- govreportst[.]com
- iceerd[.]com
- login-googlemail[.]com
- mail-redirect.com[.]kz
- mfa-events[.]com
- msoficceupdate[.]com
- officemicroupdate[.]com

- officeonlaine[.]com
- osc-e[.]com
- pwdrecover[.]com
- suporteng[.]com
- un-booklet[.]com
- update-app[.]top
- usaid[.]info
- us-embassy-report[.]com
- worlwidesupport[.]top

The activity described in this blog was derived from the ATLAS Intelligence Feed and original research by the ASERT Team. The indicators and signatures related to the activity enable Arbor APS to block the activity.

Posted In

Uncategorized

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.