XtremeRAT: Nuisance or Threat?

Rather than building custom malware, many threat actors behind targeted attacks use publicly or commercially available remote access Trojans (RATs). This pre-built malware has all the functionality needed to conduct cyber espionage and is controlled directly by humans, who have the ability to adapt to network defenses. As a result, the threat posed by these RATs should not be underestimated.

However, it is difficult to distinguish and correlate the activity of targeted threat actors based solely on their preference to use particular malware — especially, freely available malware. From an analyst's perspective, it is unclear whether these actors choose to use this type of malware simply out of convenience or in a deliberate effort to blend in with traditional cybercrime groups, who also use these same tools.

There are numerous RATs available for free and for purchase in online forums, chat rooms and market places on the Internet. Most RATs are easy to use and thus attract novices. They are used for a variety of criminal activity, including "sextortion". [1] The ubiquity of these RATs makes it difficult to determine if a particular security incident is related to a targeted threat, cybercrime or just a novice "script kiddie" causing a nuisance.

Although publicly available RATs are used by a variety of operators with different intents, the activity of particular threat actors can still be tracked by clustering command and control server information as well as the information that is set by the operators in the builder. These technical indicators, combined with context of an incident (such as the timing, specificity and human activity) allow analysts to assess the targeted or non-targeted nature of the threat.

In this post, we examine a publicly available RAT known as XtremeRAT. This malware has been used in targeted attacks as well as traditional cybercrime. During our investigation we found that the majority of XtremeRAT activity is associated with spam campaigns that typically distribute Zeus variants and other banking-focused malware. Why have these traditional cybercrime operators begun to distribute RATs? This seems odd, considering RATs require manual labor as opposed to automated banking Trojans.

Based on our observations we propose one or more of the following possible explanations:

1. Smokescreen
   The operations may be part of a targeted attack that seeks to disguise itself and its possible targets, by using spam services to launch the attacks.
2. Less traditional tools available
   With more crimeware author arrests and/or disappearance of a number of banking Trojan developers, cybercriminals are resorting to using RATs to manually steal data, such as banking and

credit card details. [2]

3. Complicated defenses require more versatile tools
   As many traditional banking and financial institutions have improved their security practices, perhaps attackers have had a much more difficult time developing automation in their Trojans to cover all variations of these defenses; as such, RATs provide more versatility and effectiveness, at the expense of scalability.
4. Casting a wider net
   After compromising indiscriminate targets, attackers may dig deeper into specific targets of interest and/or sell off the access rights of the victims' systems and their data to others.

These possible explanations are not mutually exclusive. One or all of them may be factors in explaining this observed activity.

XtremeRAT

The XtremeRAT was developed by "xtremecoder" and has been available since at least 2010. Written in Delphi, the code of XtremeRAT is shared amongst several other Delphi RAT projects including SpyNet, CyberGate, and Cerberus. The RAT is available for free; however, the developer charges 350 Euros for the source code. Unfortunately for xtremecoder, the source code has been leaked online. The current version is Xtreme 3.6, however, there are a variety of "private" version of this RAT available as well. As such, the official version of this RAT and its many variants are used by a wide variety of actors.

XtremeRAT allows an attacker to:

- Interact with the victim via a remote shell
- Upload/download files
- Interact with the registry
- Manipulate running processes and services
- Capture images of the desktop
- Record from connected devices, such as a webcam or microphone

Moreover, during the build process, the attacker can specify whether to include keylogging and USB infection functions.

Extracting Intelligence

XtremeRAT contains two components: a "client" and a "server"; however, from the attacker's perspective, these terms have reversed meanings. Specifically, according to the author, the "server" component is the malware that resides on victim endpoints that connect to the "client", which is operated by the attacker from one or more remote command-and-control (CnC) systems. Due to this confusing and overloaded terminology, we refer to the “server” as a “backdoor” on the victim and the “client” as a remote “controller” operated by the attacker.

XtremeRAT backdoors maintain and reference configuration data that was chosen by the attacker at the time they were built. This data can contain very useful hints to help group attacks and attribute them to actors, similar to what we have previously described in our Poison Ivy whitepaper. [3]

Several versions of XtremeRAT write this configuration data to disk under `%APPDATA%\Microsoft\Windows`, either directly, or to a directory named after mutex configured by the attacker. When written to disk, the data is RC4 encrypted with a key of either “CYBERGATEPASS” or “CONFIG” for the versions we have analyzed. In both cases, the key is Unicode. The config file has either a “.nfo” or “.cfg” extension depending on the version. XtremeRAT’s key scheduling algorithm (KSA) implementation contains a bug wherein it only considers the length of the key string, not including the null bytes between each character, as is found in these Unicode strings. *As a result, it only effectively uses the first half of the key*. For example, the key “`C\x00O\x00N\x00F\x00I\x00G\x00`” is 12 bytes long, but the length is calculated as only being 6 bytes long. Because of this, the key that is ultimately used is “`C\x00O\x00N\x00`”.

The configuration data includes:

- Name of the installed backdoor file
- Directory under which the backdoor file is installed
- Which process it will inject into (if specified)
- CnC information
- FTP information for sending stolen keystroke data to
- Mutex name of the master process,
- ID and group name which are used by the actors for organizational purposes

Because the decrypted configuration data can be reliably located in memory (with only slight variations in its structure from version to version) and because not all versions of XtremeRAT will write their configuration data to disk, parsing memory dumps of infected systems is often the ideal method for extracting intelligence.

We are releasing python scripts we have developed to gather the configuration details for various versions of XtremeRAT from both process memory dumps and the encrypted configuration file on disk. The scripts are available at https://github.com/fireeye/tools/tree/master/malware/Xtreme%20RAT.

Also included in this toolset is a script that decrypts and prints the contents of the log file created by

XtremeRAT containing victim keystroke data. This log file is written to the same directory as the config file and has a “.dat” extension. Curiously, this log file is encrypted with a simple two-byte XOR instead of RC4. Later in this blog, we will share some of the configuration details we have extracted during our subsequent analysis.

XtremeRAT Activity

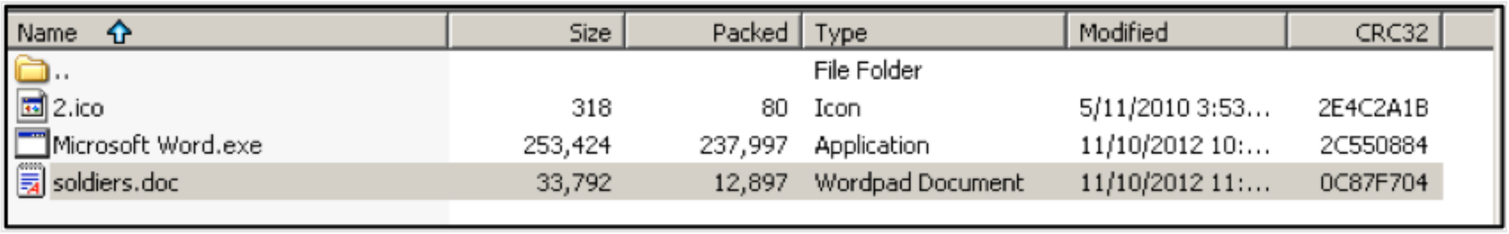
Using telemetry from the FireEye Dynamic Threat Intelligence (DTI) cloud, we examined 165 XtremeRAT samples from attacks that primarily hit the following sectors:

- Energy, utilities, and petroleum refining
- Financial Services
- High-tech

These incidents include a spectrum of attacks including targeted attacks as well as indiscriminate attacks. Among these XtremeRAT-based attacks, we found that 4 of the 165 samples were used in targeted attacks against the High-Tech sector by threat actors we have called “MoleRats”. [4]

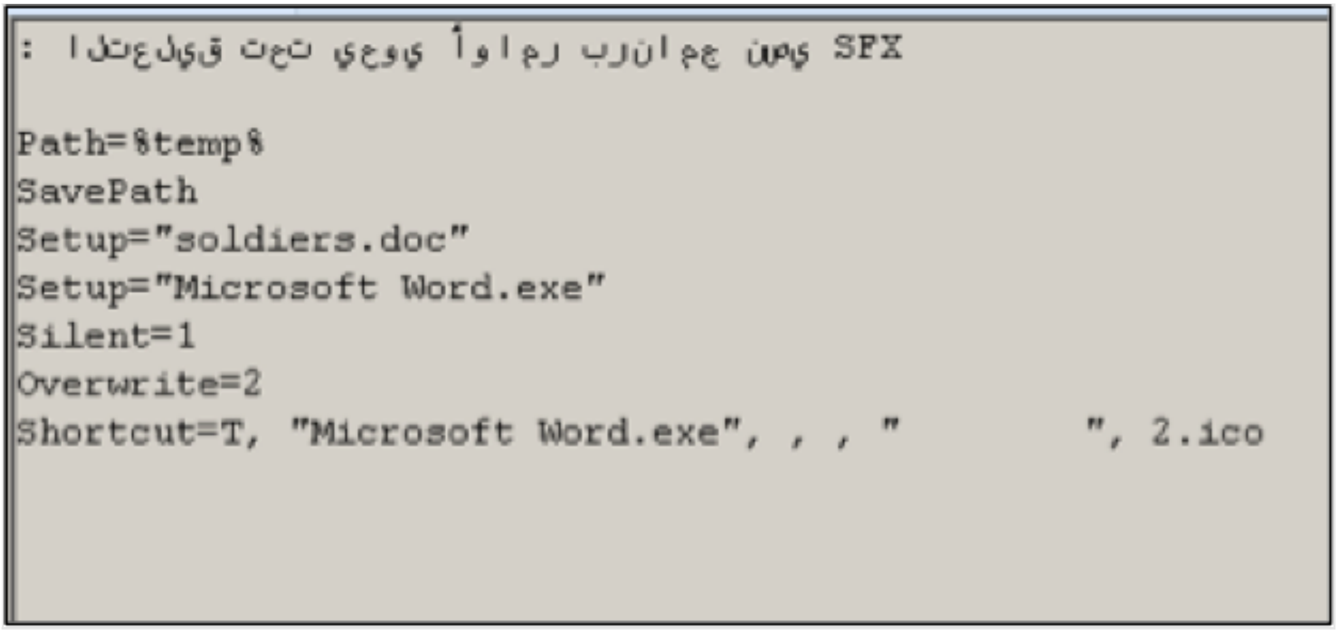
Operation Molerats

In 2012, XtremeRAT was used against a variety of governments as well as Israeli and Palestinian targets in what was known as Operation Molerats (the same attackers have also used variants of the Poison Ivy RAT). [5] Upon executing one particular sample (45142b17abd8a17a5e38305b718f3415), the malware beacons to “test.cable-modem.org” and “idf.blogsite.org”. In this particular case, the attacker used XtremeRAT 2.9 within a self-extracting archive that also presents a decoy document to the victim, where the decoy content appears to have been copied from a website.



Name	Size	Packed	Type	Modified	CRC32
..			File Folder		
2.ico	318	80	Icon	5/11/2010 3:53...	2E4C2A1B
Microsoft Word.exe	253,424	237,997	Application	11/10/2012 10:...	2C550884
soldiers.doc	33,792	12,897	Wordpad Document	11/10/2012 11:...	0C87F704

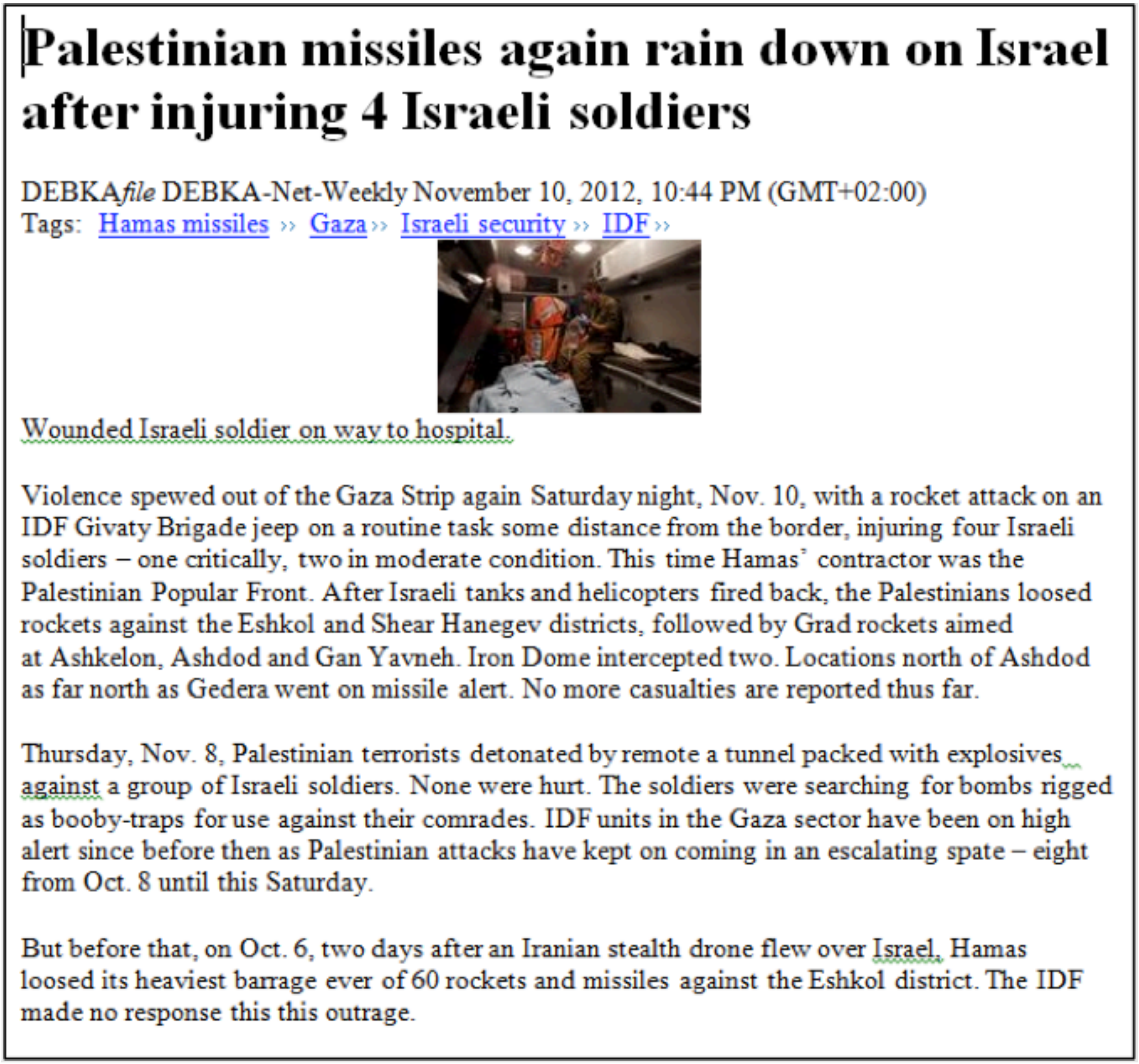
Figure 1. Contents of SFX archive containing XtremeRAT



```
: التعليق تحت يحوي أوامر برنامج نص SFX

Path=%temp%
SavePath
Setup="soldiers.doc"
Setup="Microsoft Word.exe"
Silent=1
Overwrite=2
Shortcut=T, "Microsoft Word.exe", , , "         ", 2.ico
```

Figure 2. SFX settings inside malicious archive



Palestinian missiles again rain down on Israel after injuring 4 Israeli soldiers

DEBKA*file* DEBKA-Net-Weekly November 10, 2012, 10:44 PM (GMT+02:00)
Tags: Hamas missiles ›› Gaza ›› Israeli security ›› IDF ››

Wounded Israeli soldier on way to hospital.

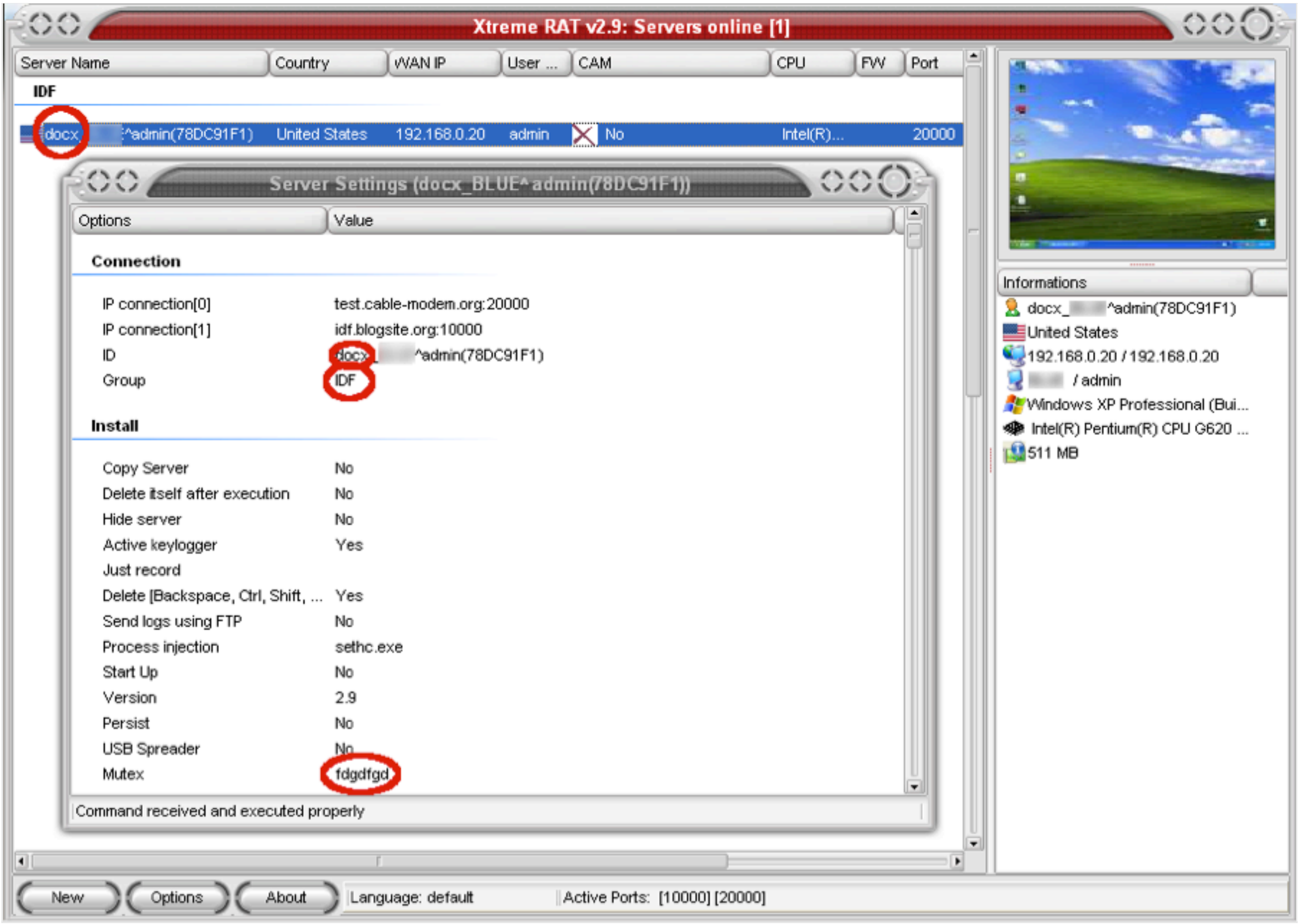
Violence spewed out of the Gaza Strip again Saturday night, Nov. 10, with a rocket attack on an IDF Givaty Brigade jeep on a routine task some distance from the border, injuring four Israeli soldiers – one critically, two in moderate condition. This time Hamas' contractor was the Palestinian Popular Front. After Israeli tanks and helicopters fired back, the Palestinians loosed rockets against the Eshkol and Shear Hanegev districts, followed by Grad rockets aimed at Ashkelon, Ashdod and Gan Yavneh. Iron Dome intercepted two. Locations north of Ashdod as far north as Gedera went on missile alert. No more casualties are reported thus far.

Thursday, Nov. 8, Palestinian terrorists detonated by remote a tunnel packed with explosives against a group of Israeli soldiers. None were hurt. The soldiers were searching for bombs rigged as booby-traps for use against their comrades. IDF units in the Gaza sector have been on high alert since before then as Palestinian attacks have kept on coming in an escalating spate – eight from Oct. 8 until this Saturday.

But before that, on Oct. 6, two days after an Iranian stealth drone flew over Israel, Hamas loosed its heaviest barrage ever of 60 rockets and missiles against the Eshkol district. The IDF made no response this this outrage.

Figure 3. Decoy content presented in malicious archive

Figure 4 shows the controller the attacker uses to interact with systems compromised with XtremeRAT. In this case, it appears the actor used the **ID** field to record the type of attack delivered (docx) and the **Group** field was used to record a “campaign code” (IDF), which helps the actor keep track of the set of victims that were attacked during this campaign.



Server Name	Country	WAN IP	User ...	CAM	CPU	FW	Port
IDF							
docx[redacted]^admin(78DC91F1)	United States	192.168.0.20	admin	☒ No	Intel(R)...		20000

Server Settings (docx_BLUE^admin(78DC91F1))

Options	Value
Connection	
IP connection[0]	test.cable-modem.org:20000
IP connection[1]	idf.blogsite.org:10000
ID	docx_[redacted]^admin(78DC91F1)
Group	IDF
Install	
Copy Server	No
Delete itself after execution	No
Hide server	No
Active keylogger	Yes
Just record	
Delete [Backspace, Ctrl, Shift, ...	Yes
Send logs using FTP	No
Process injection	sethc.exe
Start Up	No
Version	2.9
Persist	No
USB Spreader	No
Mutex	fdgdfgd

Command received and executed properly

Informations

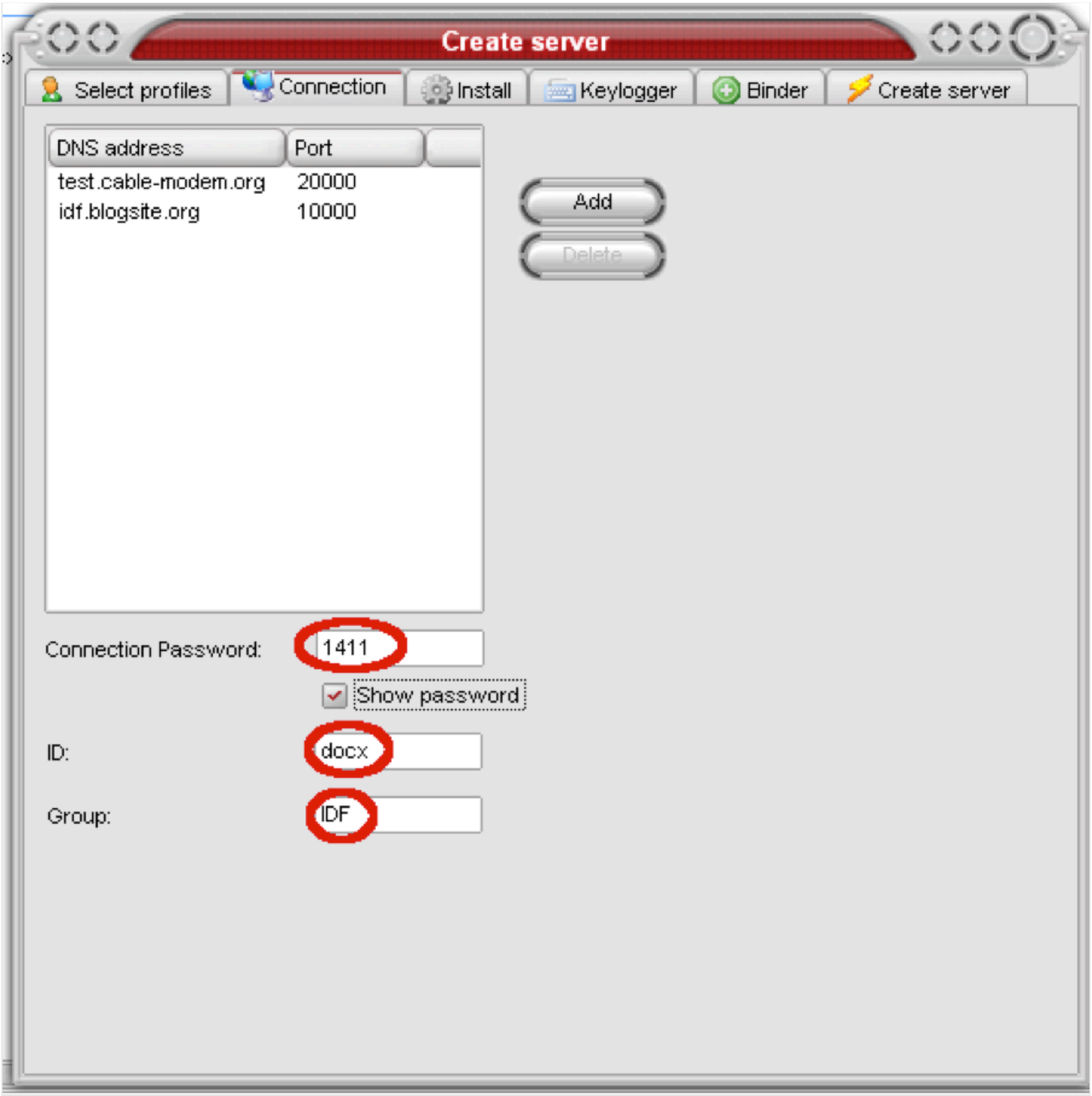
docx_[redacted]^admin(78DC91F1)
United States
192.168.0.20 / 192.168.0.20
[redacted] / admin
Windows XP Professional (Bui...
Intel(R) Pentium(R) CPU G620 ...
511 MB

Language: default

Active Ports: [10000] [20000]

Figure 4. XtremeRAT controller GUI

The attacker modified the highlighted information at build time. By default, the XtremeRAT controller sets the **ID** field as “Server” and **Group** field as “Servers”, with the default password used to authenticate, connect, and control a compromised endpoint as “1234567890”.



DNS address	Port
test.cable-modem.org	20000
idf.blogsite.org	10000

Connection Password: 1411

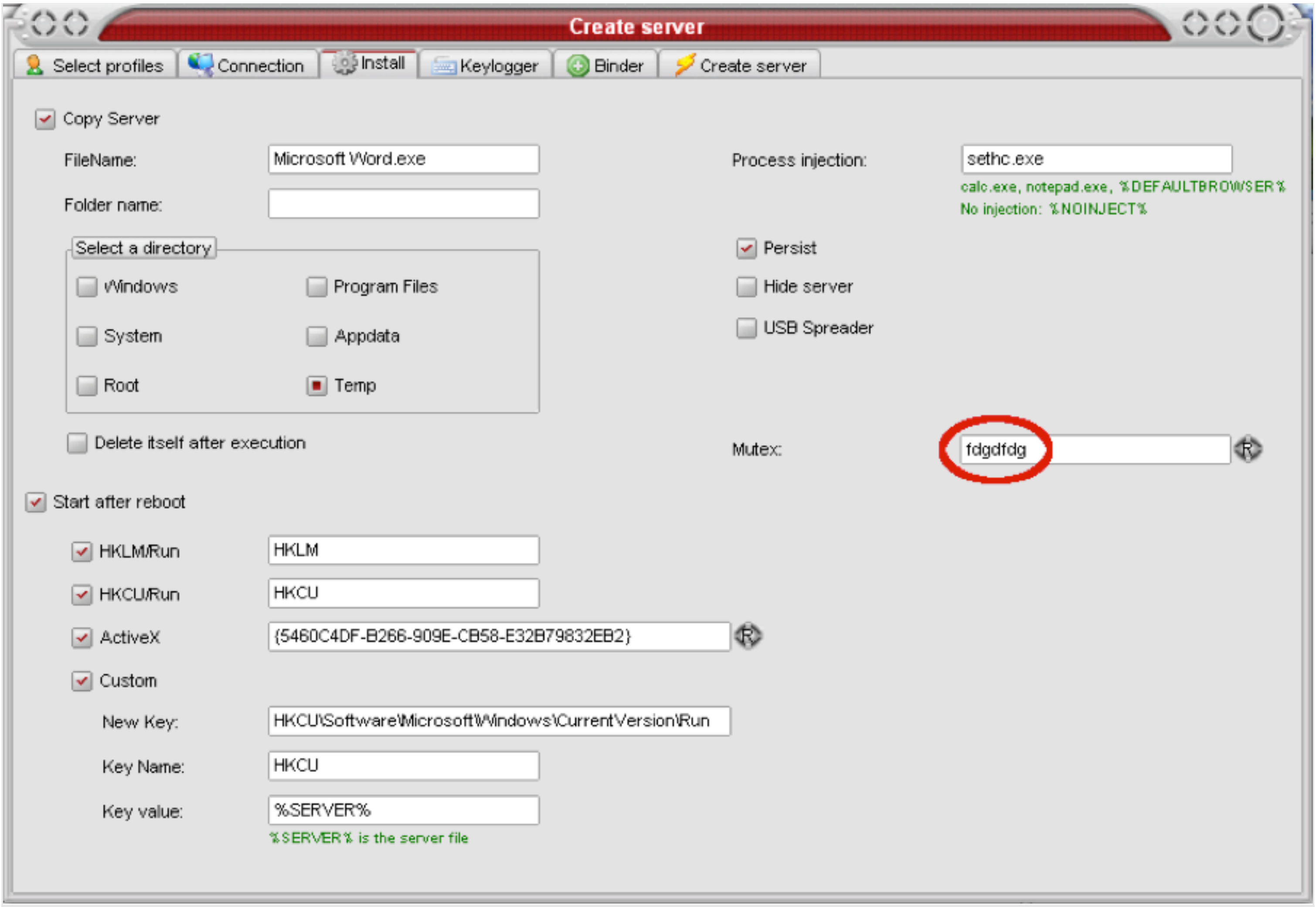
☑ Show password

ID: docx

Group: IDF

Figure 5. XtremeRAT controller connection settings

In the Figure 5, the attacker specified custom CnC servers and ports and changed the default password to “1411”. The attacker also changed the default process mutex name.



☑ Copy Server

FileName: Microsoft Word.exe

Folder name:

Select a directory

□ Windows □ Program Files

□ System □ Appdata

□ Root ■ Temp

□ Delete itself after execution

☑ Start after reboot

☑ HKLM/Run HKLM

☑ HKCU/Run HKCU

☑ ActiveX {5460C4DF-B266-909E-CB58-E32B79832EB2}

☑ Custom

New Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Key Name: HKCU

Key value: %SERVER%

%SERVER% is the server file

Process injection: sethc.exe

calc.exe, notepad.exe, %DEFAULTBROWSER%

No injection: %NOINJECT%

☑ Persist

□ Hide server

□ USB Spreader

Mutex: fdgdfdg

Figure 6. XtremeRat install settings

By default, the controller assigns a process mutex name of is "–((Mutex))–" and the attackers changed it to "fdgdfdg". These indicators along with command and control domain names and the IP addresses that they resolve to can be used to cluster and track this activity over time.

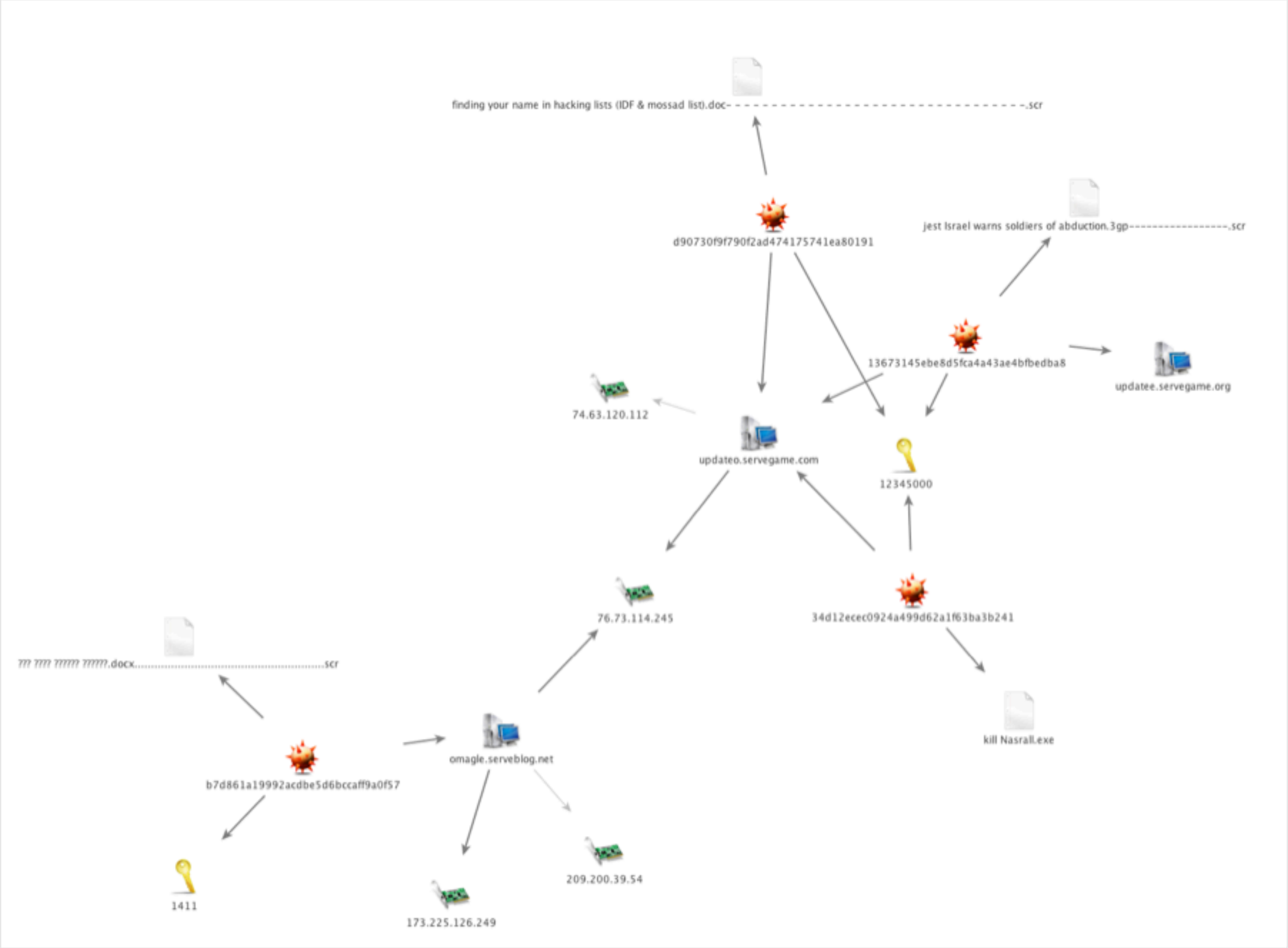

finding your name in hacking lists (IDF & mossad list).doc- -.scr
d90730f9f790f2ad474175741ea80191
jest Israel warns soldiers of abduction.3gp-----------------.scr
13673145ebe8d5fca4a43ae4bfbedba8
updatee.servegame.org
74.63.120.112
updateo.servegame.com
12345000
76.73.114.245
34d12ecec0924a499d62a1f63ba3b241
??? ???? ?????? ??????.docx..scr
kill Nasrall.exe
b7d861a19992acdbe5d6bccaff9a0f57
omagle.serveblog.net
1411
209.200.39.54
173.225.126.249

Figure 7. Molerats cluster analysis

This is a cluster of Molerats activity. In addition to using the password “1411”, the attackers are also using the password “12345000”. This is a simple way to track the activity of these actors by using both passive DNS data and configuration information extracted from XtremeRAT.

Spam Activity

The vast majority of XtremeRAT activity clustered around the default password “1234567890” (116 samples). There was overlap between this large cluster and the second largest one which used the password “123456” (12 samples). The activity in these two clusters aligns with indicators observed in Spanish language spam runs. The “123456” cluster also contains spam in the English language, leveraging the recent tragedy in Kenya as a lure. [7]

The Uranio Cluster

In our sample set, we have 28 malware samples that connect to a set of sequentially numbered command

and control servers:

- uranio.no-ip.biz
- uranio2.no-ip.biz
- uranio3.no-ip.biz
- uranio4.no-ip.biz
- uranio5.no-ip.biz
- uranio6.no-ip.biz
- uranio7.no-ip.biz
- platino.no-ip.biz
- platino-2.no-ip.biz
- platino-4.no-ip.biz
- platino-5.no-ip.biz
- platino-8.no-ip.biz
- platino-9.no-ip.biz
- cometa3.no-ip.biz
- cometa4.no-ip.biz

The malware is being spammed out and has file names such as:

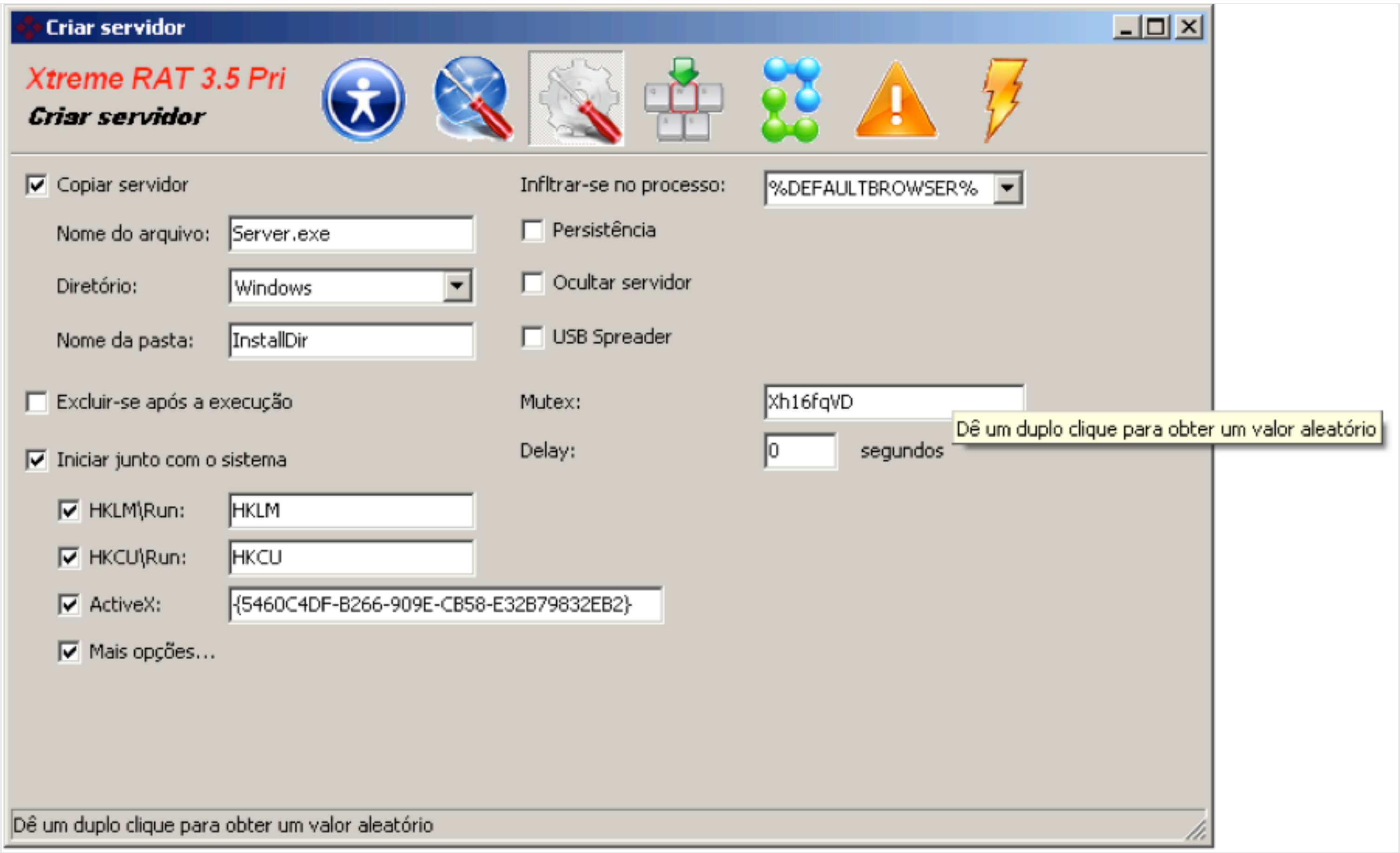
- Certificaciones De Pagos Nominas Parafiscales jpg 125420215 58644745574455 .exe
- Soportes de pagos certificaciones y documentos mes mayo 30 2013 567888885432235678888888123456.exe
- Certificaciones De Pago Y Para Fiscales.exe

We extracted the configurations for a sampling of the XtremeRAT samples we came across in this spam run and found the following results:

MD5	ID	Group	Version	Mutex
a6135a6a6346a460792ce2da285778b1	ABRIL	CmetaS3	3.6 Private	C5AapWKh
988babfeec5111d45d7d7eddea6daf28	ABRIL	CmetaS3	3.6 Private	C5AapWKh
715f54a077802a0d67e6e7136bcbe340	ABRIL	CmetaS3	3.6 Private	C5AapWKh
167496763aa8d369ff482c4e2ca3da7d	ABRIL	CmetaS3	3.6 Private	C5AapWKh
3f288dfa95d90a3cb4503dc5f3d49c16	Server	Cometa4	3.6 Private	4QtgfoP
6a8057322e62c569924ea034508068c9	Server	Platino4	3.6 Private	mbojnXS
37b90673aa83d177767d6289c4b90468	Server	Platino4	3.6 Private	mbojnXS

98fb1014f6e90290da946fdbca583334	Server	Platino8	3.6 Private	G7fjZQYAH
5a9547b727f0b4baf9b379328c797005	Server	Platino8	3.6 Private	G7fjZQYAH
fb98c8406e316efb0f46024f7c6a6739	Server	Platino9	3.6 Private	kUHwdc8Y
64f6f819a029956b8aeafb729512b460	Server	Uranio	3.6 Private	eYwJ6QX0i
a4c47256a7159f9556375c603647f4c2	Mayo	Uranio2011	3.6 Private	0pg6ooH
62d6e190dcc23e838e11f449c8f9b723	Mayo	Uranio2011	3.6 Private	0pg6ooH
d5d99497ebb72f574c9429ecd388a019	Mayo	Uranio2011	3.6 Private	0pg6ooH
3a9237deaf25851f2511e355f8c506d7	Server	Uranio3	1.3.6.16	QwcgY0a
c5e95336d52f94772cbdb2a37cef1d33	Server	Uranio3	1.3.6.16	QwcgY0a
0ea60a5d4c8c629c98726cd3985b63c8	Server	Uranio4	1.3.6.16	xjUfrQHP6Xy
41889ca19c18ac59d227590eeb1da214	Server	Uranio4	1.3.6.16	xjUfrQHP6Xy
90e11bdbc380c88244bb0152f1142aff	Server	Uranio4	1.3.6.16	xjUfrQHP6Xy
c1ad4445f1064195de1d6756950e2ae9	Server	Uranio5	3.6 Private	R9lmAhUK
e5b781ec77472d8d4b3b4a4d2faf5761	Server	Uranio6	3.6 Private	KdXTsbjJ6
a921aa35deedf09fabee767824fd8f7e	Server	Uranio6	3.6 Private	KdXTsbjJ6
9a2e510de8a515c9b73efdf3b141f6c2	CC	Uranio7	3.6 Private	UBt3eQq0
a6b862f636f625af2abcf5d2edb8aca2	CC	Uranio7	3.6 Private	iodjmGyP3
0327859be30fe6a559f28af0f4f603fe	CC	Uranio7	3.6 Private	UBt3eQq0

“Server”, “Servers”, and “–((Mutex))–” are the defaults in the XtremeRAT controller for ID, Group, and Mutex respectively. The random mutex names in the table above can be generated by double-clicking in the Mutex field within the controller. In most cases, the number at the end of the group label is the same number used at the end of the subdomain for the CnC. In the case of “Uranio2011”, the subdomain is simply “uranio” and 2011 represents the port number used to communicate with the CnC infrastructure.



Criar servidor

Xtreme RAT 3.5 Pri

Criar servidor

☑ Copiar servidor

Nome do arquivo: Server.exe

Diretório: Windows

Nome da pasta: InstallDir

□ Excluir-se após a execução

☑ Iniciar junto com o sistema

☑ HKLM\Run: HKLM

☑ HKCU\Run: HKCU

☑ ActiveX: {5460C4DF-B266-909E-CB58-E32B79832EB2}

☑ Mais opções...

Infiltrar-se no processo: %DEFAULTBROWSER%

□ Persistência

□ Ocultar servidor

□ USB Spreader

Mutex: Xh16fqVD

Delay: 0 segundos

Dê um duplo clique para obter um valor aleatório

Dê um duplo clique para obter um valor aleatório

Figure 8. Portugese version of XtremeRAT controller

Uranio Sinkhole Analysis

We sinkholed uranio2.no-ip.biz between November 22, 2013 and January 6, 2014. During that time, 12000 unique IPs connected to the uranio2.no-ip.biz. Recall, that this number reflects only one of many command and control servers. [8]

However, estimating the number of victims this way is difficult due to DHCP lease times, which inflate the numbers, and NAT connections, which deflate the numbers. [9] As such, we counted the unique IP addresses that connected to the sinkhole on each day. The highest number of connections to this sinkhole was on Dec. 3, 2013 with 2003 connections and the lowest was Jan. 6, 2014 with 109 connections. The average number of unique IP addresses that connected to the sinkhole per day was 657.

While these IP addresses were in ranges assigned to 40 distinct countries, the vast majority of the connections to the sinkhole (92.7 percent) were from Colombia. Argentina was a distant second with 1.22 percent, followed by Venezuela with 1.02 percent, Egypt with 0.95 percent and the U.S. with 0.9 percent.

Conclusion

Determining the activity of targeted threat actors is difficult. Most of the activity associated with publicly available RATs is traditional cybercrime associated with spam runs, banking Trojans and malware distribution. However, useful indicators can be extracted from these ubiquitous RATs to track the activities of targeted threat actors (as well as cybercrime).

Tools

- https://github.com/fireeye/tools/tree/master/malware/Xtreme%20RAT

Notes:

1. http://arstechnica.com/tech-policy/2013/09/miss-teen-usas-webcam-spy-called-himself-cutefuzzypuppy/ http://arstechnica.com/tech-policy/2011/09/how-an-omniscient-internet-sextortionist-ruined-lives/

2. The group behind the Carberp banking Trojan were arrested http://www.techweekeurope.co.uk/news/carberp-botnet-leader-arrested-112205, the author of Zeus retired, http://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/, the author of SpyEye went into hiding http://www.xylibox.com/2012/03/behind-spyeye-gribodemon.html and was recently arrested http://www.wired.com/threatlevel/2014/01/spy-eye-author-guilty-plea/, FBI and Microsoft have gone after Citadel which is not off the market https://blogs.rsa.com/citadels-steward-banned-from-undergorund-venues/ http://www.microsoft.com/en-us/news/press/2013/jun13/06-05dcupr.aspx and an overview of the "Big 4" banking Trojans http://blog.kaspersky.com/the-big-four-banking-trojans/

3. http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf

4. http://www.fireeye.com/blog/technical/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html

5. http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-on-usisrael-and-other-foreign-governments/
http://download01.norman.no/whitepapers/Cyberattack_against_Israeli_and_Palestinian_targets.pdf
http://www.fireeye.com/blog/technical/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html

6. http://tools.cisco.com/security/center/viewThreatOutbreakAlert.x?alertId=30825

7. http://www.symantec.com/connect/blogs/spammers-use-kenya-terrorist-attack-spread-malware

8. We filtered out all non-XtremeRAT traffic and ensured that each of the 12000 IPs attempted to make an XtremeRAT connection.

9. https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/rajab/rajab.pdf

This entry was posted in Threat Intelligence, Threat Research by Nart Villeneuve and James T. Bennett. Bookmark the permalink.