PEERING INTO GLASSRAT

A Zero Detection Trojan from China

Authors:
Kent Backman, primary research
Jared Myers, contributing
Chris Ahearn, contributing
Maor Franco, contributing
Peter Beardmore, contributing

November 23, 2015

Content and liability disclaimer

This Research Paper is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. EMC has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. EMC shall not be responsible for any errors or omissions contained on this Research Paper, and reserves the right to make changes anytime without notice. Mention of non-EMC products or services is provided for informational purposes only and constitutes neither an endorsement nor a recommendation by EMC. All EMC and third-party information provided in this Research Paper is provided on an "as is" basis.

EMC DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, WITH REGARD TO ANY INFORMATION (INCLUDING ANY SOFTWARE, PRODUCTS, OR SERVICES) PROVIDED IN THIS RESEARCH PAPER, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.
In no event shall EMC be liable for any damages whatsoever, and in particular EMC shall not be liable for direct, special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue or loss of use, cost of replacement goods, loss or damage to data arising out of the use or inability to use any EMC website, any EMC product or service. This includes damages arising from use of or in reliance on the documents or information present on this Research Paper, even if EMC has been advised of the possibility of such damages

Published in the USA. November 23, 2015

EXECUTIVE SUMMARY

RSA Research has discovered a "zero detection" Remote Administration Tool (RAT) dubbed GlassRAT, signed with a certificate which appears to have been misappropriated from a popular software developer in China. This malware has gone under the radar for what may be several years. Telemetry and limited anecdotal reports indicate that Chinese nationals associated with large multinational corporations may be the targets of campaigns employing GlassRAT. While "transparent" to most antivirus products, GlassRAT can be detected using network forensic or endpoint tools such as RSA® Security Analytics and/or RSA® ECAT. Also presented is evidence that GlassRAT's command and control (C2) infrastructure has some historical overlap with other malicious malware campaigns that have previously targeted Asia-based organizations of geopolitical and strategic importance.

OVERVIEW

When a cyber espionage campaign is identified; the threat actors' tools, techniques, and procedures revealed; the malware now detectable by antivirus- What do the bad guys do next? History shows us that this is just part of the process. Once operations or campaigns are uncovered, the attackers have contingency plans, which can include minimally substituting only the tools in their kit that may have been detected and/or perhaps finding new victims, who are less alert to their threat. There maybe no need to change the Command and Control infrastructure or their techniques.

In very large cyber intelligence organizations, which carry a diverse list of objectives and targets, there is likely to be shared leadership, policies and procedures, infrastructure, and ample sources and libraries of advanced hacking tools (many still unexposed to researchers)- all servicing subordinate organizations with far narrower objectives.

GlassRAT has (briefly) shared C2 infrastructure with some large campaigns, identified earlier in the decade, that targeted geopolitical organizations in the Asia-Pacific region. The telemetry of GlassRAT and limited forensic samples suggest that targeting is narrowly focused.

Thus, what makes GlassRat notable is not what it is, but perhaps rather where it came from, who is using it, and for what purpose. Spoiler alert: this paper does not offer a conclusion. Rather, we believe the limited facts are worth consideration, particularly when there may-well be many more undetected / undetectable samples in the wild. Detecting the infrastructure and resulting behavior of these tools is perhaps more important when preventive defenses consistently fail. It is also crucially important to recognize the potential origins of these attacks, when detected, to better understand risks to the organization.

RSA Research looked for any similarities with other previously described malware, and exploitation campaigns. While several code similarities were found with other malware such as Taidoor[1] and Taleret[2], the most interesting overlap with GlassRAT might be in the C2 infrastructure shared with geopolitical campaigns (outlined below), which were reported earlier in this decade.

BACKGROUND

GlassRAT appears to have operated, stealthily, for nearly 3 years in some environments. Evidence indicates that Chinese nationals associated with large multinational corporations in and outside of China may be the targets of campaigns employed by GlassRat.

GlassRat employs many of the telltale signs of good, at least very effective, malware design. Its dropper is signed using a compromised certificate from a trusted and well-known publisher.[3] It deletes itself after successfully delivering its payload. Once installed, the malicious DLL file persists below the radar of endpoint antivirus.

GlassRat first came to the attention of RSA Research in February 2015 when the RSA® Incident Response team, which specializes in responding to advance threat intrusions in large enterprise networks, detected malicious traffic while investigating an incident at a multi-national firm based in the U.S. A dll sample was discovered, using RSA ECAT, on the PC of a Chinese national. There was no evidence of any dropper. Retrospective analysis on Virus Total revealed a sample submitted from Hong Kong in December 2014, which exhibited matching characteristics, but a different hash. This

[1] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf
[2] https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html
[3] The Certificate Authority (CA) that issued this certificate was informed and subsequently revoked the likely stolen code-signing certificate, after independently confirming the maliciousness of the signed code.

prompted RSA to create a Yara signature which was then fed into the RSA Research hunting capability, as well as to ECAT in the client environment.

That signature alerted several months later, in September 2015, from samples appearing to originate in China. These included two droppers, and malware that was functionally identical but with different C2. (The domains were different, but the IP's overlapped with the previous samples for a period of time.)

RSA Research has linked GlassRAT C2 to other malicious malware C2 infrastructure by way of malicious domains that pointed to common hosting. In September 2012, Dell SecureWorks reported on a cyber espionage campaign that used a RAT named Mirage (also known as MirageFox).[4] PlugX C2 hosts in these and other campaigns were enumerated[5][6] by Haruyama and Suzuki at BlackHat Asia in 2014. The threat actor group who controlled alternate009.com created C2 host records for PlugX malware targeting Mongolian government[7][8].

That same threat actor group who controlled alternate009.com created C2 host records for Mirage malware[9] targeting the Philippines military[10].

The malicious domain mechanicnote.com was used for C2 by several different types of malware, including Mirage malware[11] used for targeting the Philippine military. This malware with mechanicnote.com domain C2 used a controller on the same IP address and server also used for GlassRAT malware C2 (101.55.x.x, bits.foryousee.net).

The domain news-google.net employed by MagicFire malware[12] C2 targeting the Philippine military, also used a malware controller hosted on the IP address 173.231.x.x, which was used for Mongolia-targeting PlugX malware[13] employing the malicious cainformations.com domain. Another mecahnicnote.com C2 URL used the same IP address, 198.40.x.x, as did malware using cainformations.com and alternate009.com domains for C2. These domains in turn are tied directly to Magicfire, Mirage and PlugX malware in several malicious campaigns.

To summarize the GlassRAT C2 infrastructure connections, we have GlassRAT connected to Mirage malware C2 hosting, which in turn is connected to Magicfire, PlugX and Mirage malware targeting the Philippine military and the Mongolia government. The temporal overlap window in shared infrastructure was relatively short implying a possible operational security slip by the actors behind GlassRAT if not deliberate sharing of infrastructure. The infrastructure overlap traced by RSA Research can be seen in detail in the attached C2 overlap graphic in the Appendix.

[4] http://www.secureworks.com/cyber-threat-intelligence/threats/the-mirage-campaign/
[5] https://www.blackhat.com/docs/asia-14/materials/Haruyama/Asia-14-Haruyama-I-Know-You-Want-Me-Unplugging-PlugX.pdf
[6] http://pastebin.com/B2jNMrM8
[7] https://www.threatconnect.com/khaan-quest-chinese-cyber-espionage-targeting-mongolia/
[8] http://pastebin.com/B2jNMrM8
[9] https://www.virustotal.com/en/file/421f4c83898ff3ae9b2a94621140ef770888a8a0914b163cdae4690433173899/analysis/
[10] http://blog.trendmicro.com/trendlabs-security-intelligence/christmas-themed-malware-starts-to-jingle-all-the-way/
[11] https://www.virustotal.com/en/file/91279f578d2836ea679ae9578068cb70810fb781faf6d7c03c3212aa509f3e7b/analysis/
[12] https://www.virustotal.com/en/file/2ee38b14a570f693c093a53c53c6d10234fb11cfb7318022190cdb8c96d73b35/analysis/
[13] http://pastebin.com/B2jNMrM8

DROPPER SUBMISSIONS FROM CHINA

As discussed above, RSA Research was first alerted to some specific zero detection malware by the RSA Incident Response services team. Also notable is that the first observed sample[14] of this zero detection malware may have been deployed since September of 2012, if the compile time (Figure 1) is any indicator. We don't know if there is any connection between the compilation of GlassRAT and the reports of malware outlined above, much occurring in roughly the same timeframe.

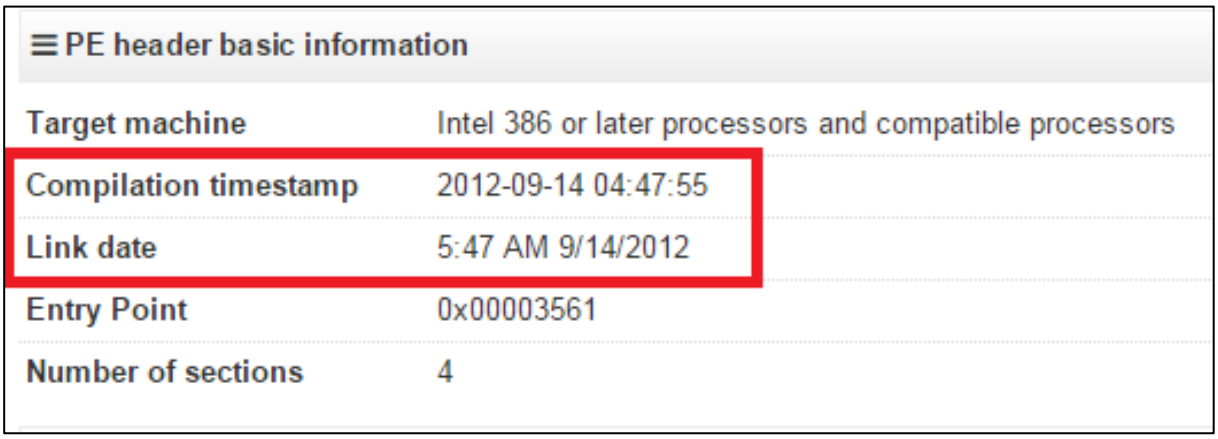


Figure 1 Compilation timestamp of first known sample of GlassRAT malware, appearing on VirusTotal in September of 2014.

The indicators (see GlassRAT Yara signature in appendix) were fed into the RSA Research hunting capability. Months later; RSA Research was alerted to two samples of the GlassRAT malware installer program or "dropper." Both of these dropper samples were not detected by static analysis routines of 57 different Antivirus vendors (Figure 2) on the VirusTotal website.

Figure 2 Zero Antivirus detection ratio of GlassRAT dropper

The two GlassRAT malware dropper samples were functionally identical. One of the samples was uploaded to VirusTotal about four hours before the next dropper[15]. The second GlassRAT dropper for which RSA Research was alerted[16] was signed with a valid code-signing certificate associated with a Beijing-based software developer. One particular application associated with this developer has over half a billion users worldwide, according to the company.

[14] https://www.virustotal.com/en/file/89317809806ef90bb619a4163562f7db3ca70768db706a4ea483fdb370a79ede/analysis/
[15] https://www.virustotal.com/en/file/c11faf7290299bb13925e46d040ed59ab3ca8938eab1f171aa452603602155cb/analysis/
[16] https://www.virustotal.com/en/file/30d26aebcee21e4811ff3a44a7198a5c519843a24f334880384a7158e07ae399/analysis/

UNDER THE RADAR FOR YEARS, TARGETS CHINESE NATIONALS OR ORGANIZATIONS

Also notable is that the first publically accessible sample of this zero-detection malware (Figure 3) may have been in the wild since September of 2012, if the compile time is any indicator. RSA Research has no reason to suspect that the compile date was forged. Additionally, RSA has learned through telemetry data and limited anecdotal reports that GlassRAT may principally be targeting Chinese nationals or other Chinese speakers, in China and elsewhere, since at least early 2013. The samples uploaded on 24 September 2015 appear to be the first known instance of the dropper/installer files.

Figure 3 First sample of GlassRAT known in the wild

The absence of an identified dropper in public malware databases prior to September 2015 may explain why the GlassRAT Trojan has maintained a low profile with AV vendors since its first appearance on VirusTotal in December of 2014 (Figure 4).

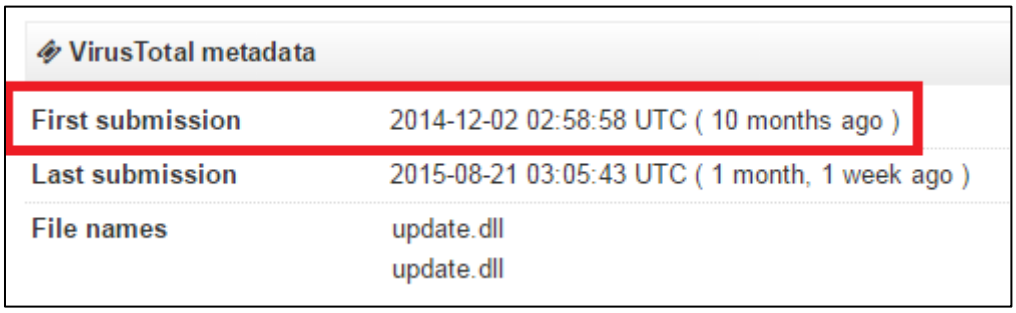
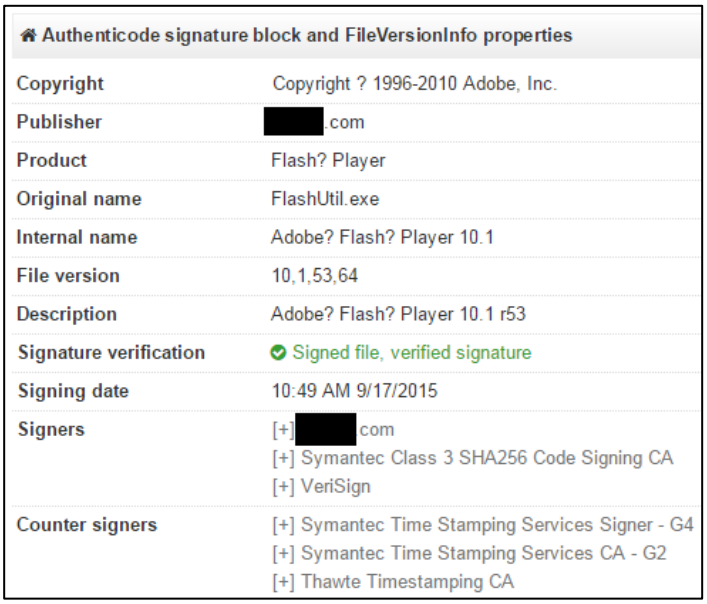


Figure 4 First submission date of identified GlassRAT malware as per VirusTotal

Figure 5 shows some of the code-signing certificate details, with the name of the software developer redacted.



Authenticode signature block and FileVersionInfo properties	
Copyright	Copyright ? 1996-2010 Adobe, Inc.
Publisher	[redacted].com
Product	Flash? Player
Original name	FlashUtil.exe
Internal name	Adobe? Flash? Player 10.1
File version	10,1,53,64
Description	Adobe? Flash? Player 10.1 r53
Signature verification	Signed file, verified signature
Signing date	10:49 AM 9/17/2015
Signers	[+] [redacted].com [+] Symantec Class 3 SHA256 Code Signing CA [+] VeriSign
Counter signers	[+] Symantec Time Stamping Services Signer - G4 [+] Symantec Time Stamping Services CA - G2 [+] Thawte Timestamping CA

Figure 5 GlassRAT signed file metadata

At the time of this writing, the malware has been shared with Symantec and Adobe, who were indirectly effected because of the Adobe trademark and the Symantec/Verisign certificate. As more vendors are made aware of this malware, RSA Research believes the detection ratio will increase from the near zero ratio at the time of this writing.

GLASSRAT MALWARE ANALYSIS, DESIGNED FOR DECEPTION

RSA's Research has analyzed the GlassRAT trojan and determined that it is a simple but capable RAT with reverse shell as well as other typical capabilities of RATs, such as file transferring and process listing. The GlassRAT dropper uses the trademarked icon of Adobe Flash player, and was named "Flash.exe" (Figure 6) when it was uploaded to VirusTotal from an IP address, likely in the Peoples Republic of China on September 17, 2015.

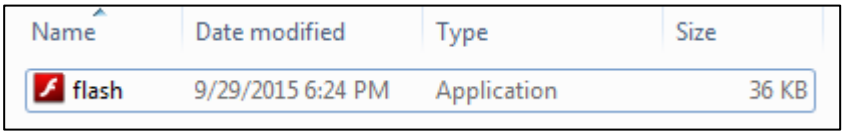


Figure 6 GlassRAT dropper as viewed in Windows Explorer

Double clicking on the flash.exe files causes the dropper to launch. The GlassRAt malware installation is as follows:

1. Dropper (flash.exe) writes the GlassRAT DLL to the ProgramData folder
2. Dropper runs the DLL file using the built-in Windows utility rundll32.exe
3. GlassRAT DLL file modifies the run key for logon persistence with user-level permissions with the following registry key.

   `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` **`Update`**

4. the dropper deletes itself with and embedded command:

   `"cmd.exe /c erase /F "%s","`

While the DDL file is actually written to the root of "C:\ProgramData" the registry entry points to the legacy junction in Windows Vista and later "C:\ProgramData\Application Data\" as would be shown in the Microsoft SysInternals Autoruns tool.

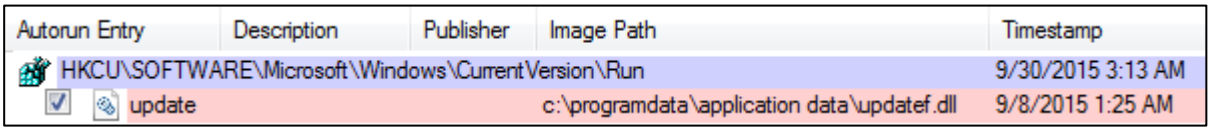


Figure 7 GlassRAT non-privileged persistence as viewed through the Autoruns tool

Manually bypassing UAC with a right-click reveals metadata associated with the dropper (Figure 8).

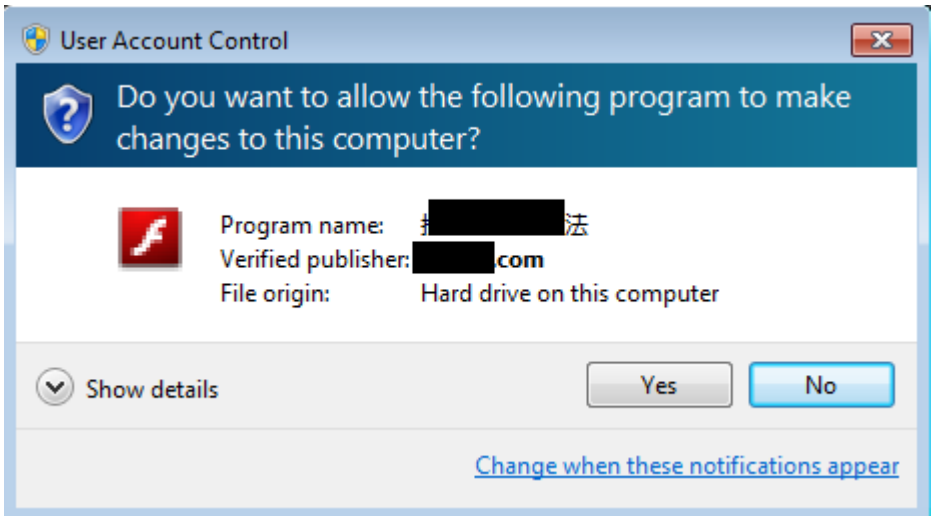


Figure 8 UAC pop-up if invoked with right click and "Run as administrator"

The program name text presented in the UAC dialog box is identical to the name of the legitimate "500 million-user" application produced by the owner of the certificate.

In the case of installation with privileged user rights such as might be obtained by an exploit or particularly good social engineering technique, persistence would consist of installation as an unused service (such as the "RasAuto" service in Figure 9), which is commonly a disabled-by-default service on ordinary Windows user/client PC's.

HKLM\System\CurrentControlSet\Services c:\programdata\application data\updatef.dll

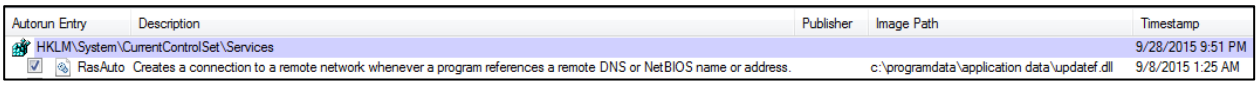


Figure 9 GlassRAT persistence mechanism if installed using administrative privileges

The timestamp on the DLL reflects the compile date of the binary.

RSA Research found samples of GlassRAT with three unique C2 configurations (Table 1). Static analysis of these GlassRAT DLL's revealed that the C2 host configuration is obfuscated in all of the samples using a simple XOR technique, utilizing 0x01 as the one-byte key. The most recent sample used URL's for C2, other samples used URL's in combination with a hard coded IP address (perhaps as a backup), and yet another GlassRAT sample we found used only a single IP address with no URLs. The C2 port for each specified C2 node is stored as a packed string and can be readily decoded with a simple script.

GlassRAT DLL MD5	Obfuscated C2 hosts(s)	C2 hosts XOR decoded with 0x01
5c17395731ec666ad0056d3c88e99c4d	003/064/50/60	112.175.x.x
e98027f502f5acbcb5eda17e67a21cdc	chur/gnsxntrdd/odu 012/31/084/353	bits.foryousee.net 103.20.x.x
59b404076e1af7d0faae4a62fa41b69f	py/s`trdsr/bnl ly/s`trdsr/bnl yy/s`trdsr/bnl	qx.rausers.com mx.rausers.com xx.rausers.com

Table 1 Three different GlassRAT C2 host configurations found in the wild by RSA Research

GLASSRAT CAPABILITIES AND FUNCTIONS

GlassRAT provides reverse shell functionality to an infected victim. The communication contains a handshake between the attacker and the victim. The sample will send the hard coded value 0x cb ff 5d c9 ad 3f 5b a1 54 13 fe fb 05 c6 22, the response from the C2 is then compared with the value 0x3f5ba154 and then the subsequent commands are a series of two byte codes. The malware performs a sanity check to make sure that the low byte of the two-byte combinations is 17 (0x11) or less. A QWORD is used to track directionality, and a DWORD is used to delimit data size. Control data is then passed to and from GlassRAT in the clear, such that system information and Windows command shell output would be readily observable in network traffic. GlassRAT initially accepts two primary commands (both with a set of sub commands) from its controller which are as follows:

0x01: Provides/Enumerates system information from the victim host
0x02: Native Command and reverse shell communications and output.

The initial beacon and handshake of controller-initiated C2 will pass the IP address of the victim to the GlassRAT controller. However, this was not observed in our dynamic analysis, suggesting that it requires manual command from the C2 operator. Perhaps such commands are performed by the operator only if a connection by a nosy researcher has been ruled out.

When the 0x01 primary command is issued the malware is configured with the following subcommands, which are in red.

```
0x01 01 – C2 request for System Information
0x01 02 – Victim response to request for system information
0x01 03 – C2/Victim keep alive
0x01 06 – C2 Read C:\ProgramData\off.dat
```

When the 0x02 primary command is issued the malware is configured with the following subcommands. Not all of the 17 possibilities are utilized in the samples that were analyzed, and this could allow for future expansion of the malware's capabilities by its author(s).

```
0x02 01 – C2 Cmd command
0x02 02 – Victim Response from cmd commands
0x02 03 – C2 initiate cmd.exe pipe/thread
0x02 04 – C2 kill cmd pipe/thread
0x02 05 – C2 execute file/start process
0x02 06 – Not Used/present
0x02 07 – Not Used/present
0x02 08 – Victim response to file download – File not found
0x02 09 – Not Used/present
0x02 0A – Not Used/present
0x02 0B – C2 command to get handle information
0x02 0C – Download file from Victim
0x02 0D – Victim response to file download – File transmission
```

```
0x02 0E – Upload/write file to Victim
0x02 0F – Not Used/present
0x02 10 – C2 command to get handle information
0x02 11 – Create process on Victim
0x02 12 – Victim response to file upload
```

COMMAND AND CONTROL

To perform dynamic analysis on the new dropper, RSA Research leveraged RSA Security Analytics (Figure 10) and RSA ECAT to quickly gather indicators and forensic details about the GlassRAT malware.

Figure 10 GlassRAT C2 activity in RSA® Security Analytics

RSA® ECAT (Figure 11) reveals that the Trojan is loaded as RasAuto service (via svchost.exe network service process) when installed with administrative privileges, and Figure 12 indicates detection by RSA® ECAT when installed with non-privileged credentials (rundll32.exe running the GlassRAT DLL).

svchost.exe	svchost.exe	115.144.1 [redacted] 3	qx.rausers.com	443	Tcp	☑
svchost.exe	svchost.exe	115.144.1 [redacted] 3	qx.rausers.com	80	Tcp	☑
svchost.exe	svchost.exe	115.144.1 [redacted] 3	qx.rausers.com	53	Tcp	☑

Figure 11 GlassRAT (administrative install) C2 as detected by RSA® ECAT

Process	Module	IP	Domain	Port	Listen
rundll32.exe		115.144.[redacted]	qx.rausers.com	443	☐
rundll32.exe		115.144.[redacted]	qx.rausers.com	80	☐
rundll32.exe		115.144.[redacted]	qx.rausers.com	53	☐

Figure 12 GlassRAT (user-level install) C2 as detected by RSA® ECAT

Analysts wishing to leverage RSA® ECAT to find RATs including GlassRAT in their enterprise networks may want to refer to the technical whitepaper "Catching the R.A.T. with ECAT"[17] presented at RSA Charge by Justin Lamarre.

RSA® Security Analytics reveals connections to following host aliases, which as of the time of this writing, resolve to the same IP address: 115.144.x.x in South Korea. The GlassRAT connects with the following string in the handshake.

cb ff 5d c9 ad 3f 5b a1 54 13 fe fb 05 c6 22

The handshake protocol has been incorporated into a parser for RSA® Security Analytics (Figure 13) that is included in this report's annex, as well as on RSA® Live.

Figure 13 GlassRAT C2 parser in action on RSA® Security Analytics

Even without the parser (typical with a protocol-abusing raw socket connection) RSA® Security Analytics flags on "unknown service over http port" and "unknown service over ssl port" (Figure 14), cluing the security investigator to the probability that the traffic is malicious.

[17] http://charge.rsa.com/wp-content/uploads/2015/09/Finding-The-R.A.T-With-ECAT.pdf

Figure 14 GlassRAT protocol abuse identified by Security Analytics

In each case, the Trojan dropper installed the DLL with the file pointer hard coded to be 12 megabytes in size. Thus, although the functional part of the GlassRAT DLL is only 16kb or so in size, the file size shown on disk is much larger (Figure 15).

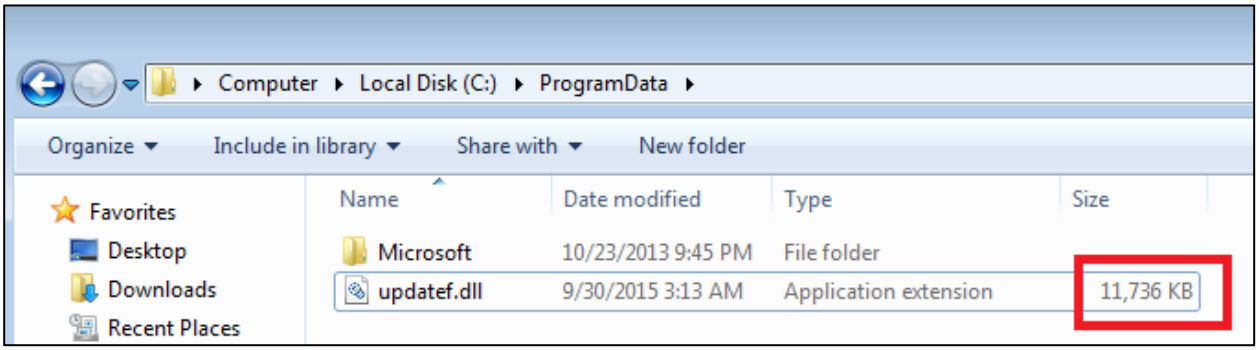


Figure 15 GlassRAT DLL takes 11+MB on disk, but consists of mostly null data bytes

APPENDIX

Campaign C2 overlap graphic

Malware hashes

C2 infrastructure (some IP addresses redacted)

GlassRAT Yara signature

PRIVATE ANNEX

Unredacted C2 infrastructure

Unredacted campaign C2 overlap graphic

GlassRAT C2 decoder script

(RSA customers and vetted industry partners can have access to the private annex by emailing conops@RSA.com.)