Detecting GlassRAT using Security Analytics and ECAT

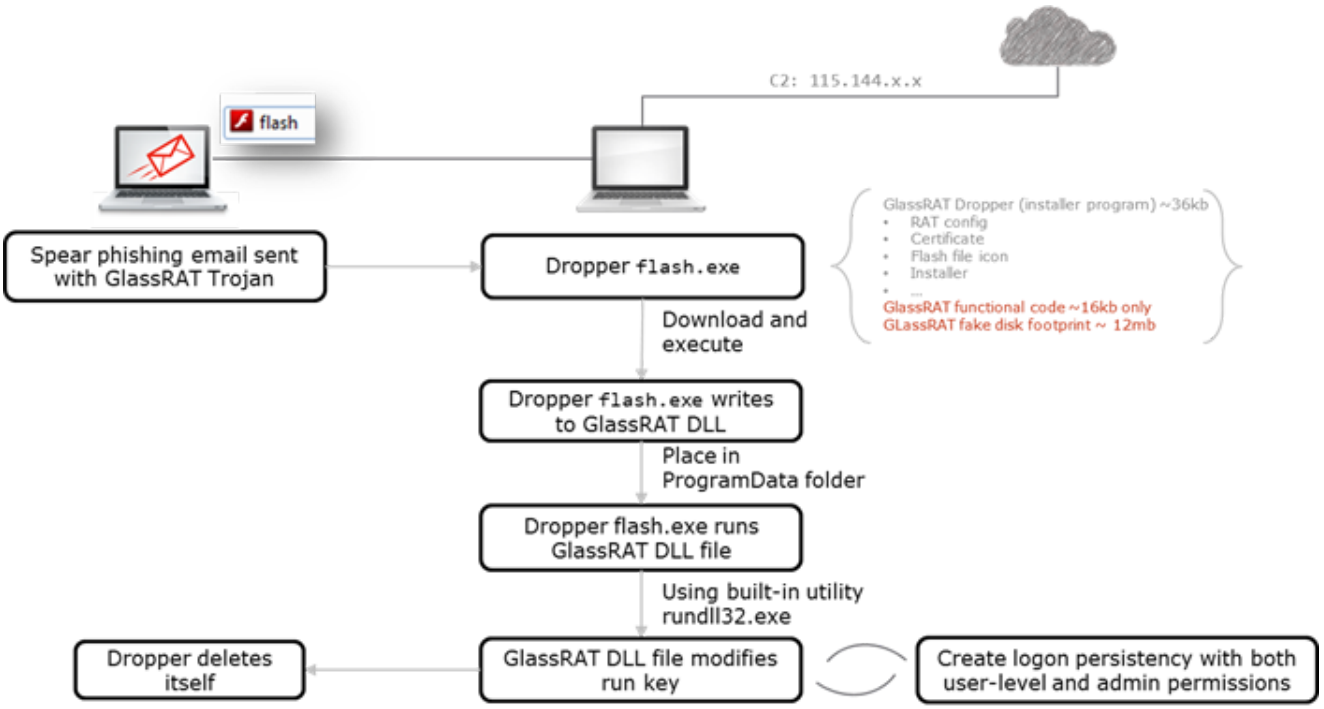
community.rsa.com/community/products/netwitness/blog/2015/11/25/detecting-glassrat-using-security-analytics-and-ecat

November 25, 2015

GlassRAT is a new zero detection Remote Access Trojan (RAT) that has been associated with different targeted attack recently, and suspected dwell time going under the radar is about several years.

In this blog post we will discuss how to detect its dropper, malicious files, and C2 communication.

Below you can see GlassRAT lifecycle from infection to persistency.



Once it infects a machine, the attacker using reverse shell is able to get access to infected victim's pc.

Once the installer program (aka "dropper") flash.exe landed and triggered on the device, it was detected by RSA ECAT and automatically been downloaded for investigation. Specifically for the dropper, there was a chain revoked alert triggered for it.

RSA ECAT Module view

File Name	IIOC Score	Machine C...	Signature	Size In Bytes	Description	Hash Lookup
flash.exe	128	1	Chain Revoked, Revoked: ...	45.3 kB	Adobe? Flash? Player 10.1 r53	Unknown

The screenshot below from RSA ECAT as well, shows how the dropper is writing the malicious code to the device creating updatef.dll

Tracking (4)

Event Time	Source File Name	Event	Target File Name
11/22/2015 11:01:19.883 PM	svchost.exe	Open Process	flash.exe
11/22/2015 11:01:19.898 PM	flash.exe	Write to Executable	updatef.dll

The screenshot below shows the network activity in RSA Security Analytics investigator beaconing out from rundll32.exe triggering new GlassRAT parser created (available in report annex and in RSA Live), and identifying infected host to C2 handshake with the following hard coded sting '0x cb ff 5d c9 ad 3f 5b a1 54 13 fe fb 05 c6 22':

Assuming the appropriate meta keys are enabled, the following query can also be used to identify the:

- Windows command shell communication: service = 0 && tcp.dstport = 80 && risk.warning = 'windows command shell'
- Protocol-abusing raw socket connection flagged as 'unknown service over http port' and 'unknown service over ssl port' under 'Risk: Informational" meta value using 'nw60125' application rule.

All of the IOCs from those HTTP sessions were added to the following RSA FirstWatch Live feeds:

- RSA FirstWatch APT Threat Domains

- RSA FirstWatch APT Threat IPs

To read the full report navigate here: https://blogs.rsa.com/peering-into-glassrat/