Digital Vengeance: Exploiting the Most Notorious C&C Toolkits

Author: Waylon Grange

Every year thousands of organizations are compromised by targeted attacks. In many cases the attacks are labeled as advanced and persistent which suggests a high level of sophistication in the attack and tools used. Many times, this title is leveraged as an excuse that the events were inevitable or irresistible, as if the assailants' skill set is well beyond what defenders are capable of. To the contrary, often these assailants are not as untouchable as many would believe.

If one looks at the many APT reports that have been released over the years some clear patterns start to emerge. A small number of Remote Administration Tools are preferred by actors and reused across multiple campaigns. Frequently sited tools include Gh0st RAT, Plug-X, and XtremeRAT among others. Upon examination, the command and control components of these notorious RATs are riddled with vulnerabilities. Vulnerabilities that can be exploited to turn the tables from hunter to hunted.

The hackers that use these RATs, often labeled nation state sponsored, enjoy a certain amount of impunity. Being titled as an advanced threat further conveys the thought that they are beyond reach and untouchable for all but the most elite. To the contrary, analysis of the tools utilized by these groups reveals they are vulnerable to remote attacks, maybe even more so than their victims. This paper hopes to break down the mythical imperceptible hacker and put them on equal ground.

Ethics of Hacking back

Of the 181 people questioned in a 2012 Black Hat survey 36% said they engaged in some form of hacking back.[1] This has been a topic of much debate in recent years, and has recently surfaced again in a US draft bill to make hacking back legal.[2] The general consensus is that most organizations have very little to gain from hacking back. Others still may want some kind of retaliation even if just for emotional reasons. Retaliation offers very little to the victims and it comes at a high risk. Beyond the ethical issues there could be civil and criminal penalties for such actions not to mention the liability, damage to reputation, costs, and loss in productivity when engaging in this generally fruitless activity.

Despite this, there are cases where hacking back can be insightful. Hacking back against attackers can provide valuable insight into the tools, techniques, and procedures used by the actor. This information can then be used to provide better attribution, detection of the group, and track their activities for whom they may be targeting. This suggests that hacking back may be of large value to threat researchers. Then again, perhaps just arming the general public with the

knowledge and capabilities needed to hack back may prove to be a strong deterrent for would be attackers.

Previous work

Some very common RATs have already been found to contain vulnerabilities. These should be presented and given credit where due.

Poison Ivy

Poison Ivy has been used in several high-profile malware campaigns, most notoriously, the 2011 compromise of RSA SecurID data. It contains a bevy of features and enjoyed a long 8 year run as one of the most notorious RATs around. Andrzej Dereszowski disclosed a buffer overflow exploit against the C2 server that provides remote code execution.[3]

After disclosure of this vulnerability researchers at malware.lu used this exploit to compromise C2 servers used by the APT1 threat group as identified by Mandiant.[4] With this access they were able to gain great visibility into the techniques and tools used by this actor. They revealed infrastructure, toolkits, and targets of this group. This case where a retaliation against an APT group has been documented shows the potential information available for researchers who hack back.

DarkComet

DarkComet is a very popular RAT that's been around since 2008 and has been used by everyone from your average script kiddie or would-be cybercriminal to 'APT-style' attackers targeting oil transportation tankers or Syrian activists. Shawn Denbow and Jesse Hertz have shown that the DarkComet C2 server is vulnerable to both an SQL injection vulnerability and an arbitrary file download vulnerability allowing an attacker to download any file from the RAT C2 server.[5]

New exploits

Gh0st Rat

Gh0st Rat is one of the most commonly referenced tools in APT reports. This tool has been used for almost 10 years and has been used against diplomatic, political, economic, and military targets. The code has been in the public for many years and there are many variants. It has a rich feature set and is a favorite amongst hacking groups in the Asia Pacific region. Since the source code is public it also lends itself to vulnerability analysis which exposes many design flaws.

There exists a logic vulnerability in the code for transferring files from the victim to the C2 Server in that there is no validation that the C2 server actually requested the file in the first place.

Furthermore, the file path where the C2 server stores the file is contained within the message from the C2 victim thus allowing an arbitrary file write on the C2 server.

This exploit can be paired with a DLL side load vulnerability in the C2 Server to allow a persistent backdoor whenever the Gh0st C2 server component is started. The DLL oledlg.dll can be side loaded when the C2 Server starts. Specifically, the only function imported from that dll is ordinal #8 (OleUIBusyA) which returns 1 on success. Since there is only this one function used and it is easy to stub out oledlg.dll it doesn't even need to be shimed and can be replaced with a specially crafted backdoor that takes care to provide the one needed function by ordinal.

Additionally, there exists a buffer overflow in the C2 Server component that handles the drive list as received from the victim that can lead to remote code execution and logic bugs that allow for arbitrary file upload. The buffer overflow is within a class structure that allows an attacker to overwrite member variables. Most promising are class variables that when overwritten are essentially a pointer to a pointer to the code the attacker would execute.

PlugX

PlugX a.k.a. Korplug, Destory RAT, or Sogu, is another notorious RAT often sited in compromises of government-related institutions. It is commonly used by groups like APT1 and Winnti. Like the other RATs it is a feature rich toolkit that is poorly written and is vulnerable to attack.

The C2 server contains multiple parsing vulnerabilities and a buffer overflow that can lead to remote execution. Ironically, the authors of this RAT even test if the data is too large for the buffer but only after that data has been copied over the buffer and the damage already done. By overwriting the return on address on the stack code execution can be gained however the code will first detect the buffer overflow and display a popup message before the return address is reached. Upon the user of the C2 Server acknowledging the popup code flow then can be controlled via the exploit. It may be possible to gain execution via other means such as SEH but little research was done looking into this.

XtremeRat

XtremeRat is a publicly available RAT that has been used in both targeted attacks and traditional cybercrime. Originally, the authors offered the RAT for free and charged for the source code but that model was broken when the source code was leaked online. Since then the code has been used in other RATs such as Spynet, CyberGate, and Cerberous. This code contains an arbitrary file download vulnerability allowing an attacker to download any file from the RAT C2 server. Although only tested in Xtreme RAT, since the code is shared between multiple RAT families the exploit may be shared amongst them as well.

Conclusions

The security posture of the RATs listed in this paper are terribly insecure and attackers are taking on substantive risk by running the software. There is no reason to believe other common RATs are any different. By design RATs like this require the C&C server to be publicly accessible which in turn exposes them to attacks from the internet at large. Since the location of these C2 servers can be extracted from the malware they are pushing, C2 servers can only remain hidden for so long. One could simply search malware repositories such as VirusTotal for implants matching these given RATs and extract C2 server information to obtain an extensive list of potential targets for counter hacking.

References:

1. Business Wire, “Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking” http://www.businesswire.com/news/home/20120726006045/en/Black-Hat-Survey-36-Information-Security-Professionals
2. Tom Graves, “Active Cyber Defense Certainty Act Draft 2.0” https://tomgraves.house.gov/uploadedfiles/discussion_draft_active_cyber_defense_certainty_act_2.0_rep._tom_graves_ga-14.pdf
3. Andrzej Dereszowski, “Targeted attacks: From being a victim to counter attacking” http://www.signal11.eu/en/research/articles/targeted_2010.pdf
4. Malware.lu, “APT1: technical backstage” https://malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf
5. Shawn Denbow & Jesse Hertz, “pest control: taming the rats” https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/PEST-CONTROL.pdf