Examining a Possible Member of the Winnti Group

blog.trendmicro.com/trendlabs-security-intelligence/pigs-malware-examining-possible-member-winnti-group/

April 19, 2017

Updated on April 26, 2017, 01:39 PM (UTC-7) to add the accurate IP address.

In one of our previous blog entries, we covered how the threat actor known as Winnti was using GitHub to spread malware – a development that shows how the group is starting to evolve and use new attack methods beyond their previous tactics involving targeted attacks against gaming, pharmaceutical, and telecommunications companies. Through this entry, in which we take a closer look at an individual who we believe might be connected to the Winnti group, we hope to give both ordinary users and organizations better insights into some of the tools – notably the server infrastructures- these kinds of threat actors use, as well as the scale in which they operate.

Searching Domain Registrations for Clues

Threat actors typically register and use several domains in order to discretely lead their malware to their Command and Control (C&C) servers. Registering a domain name always requires some form of identifying information: a physical or mailing address, an email address, and a phone number. Of these, a valid email address holds the greatest importance because it is where the registrar sends the confirmation of a domain purchase to the new owner in addition to the information needed to control the domain.

Most fraudsters create one-time email addresses or use stolen email addresses, both of which are easy to create or obtain. However, over time, it becomes tedious for fraudsters to constantly change information when registering new domains. This is the point where they are likely to make mistakes and start reusing e-mail addresses.

A careful analysis of the domain registrations from this threat actor between 2014 and 2015 allowed us to identify one profile used to register several domains that were used as C&C servers for a particular malware family employed by the Winnti group. In particular, we managed to gather details on an individual using the handle Hack520, who we believe is connected to Winnti.

Who is the Winnti group?

The group behind the Winnti malware (which we will call the Winnti group for brevity) sprung up as a band of traditional cyber crooks, comprising black hats whose technical skills were employed to perpetrate financial fraud. Based on the use of domain names they registered, the group started out in the business of fake/rogue anti-virus products in 2007. In 2009, the Winnti group shifted to targeting gaming companies in South Korea using a self-named data- and file-stealing malware.

The group, which was primarily motivated by profit, is noted for utilizing self-developed technically-proficient tools for their attacks. They once attacked a game server to illicitly farm in-game currency ("gaming gold", which also has real-world value) and stole source codes of online game projects. The group also engaged in the theft of digital certificates which they then used to sign their malware to make them stealthier. The Winnti group diversified its targets to include enterprises such as those in pharmaceutics and telecommunications. The group has since earned infamy for being involved in malicious activities associated with targeted attacks, such as deploying spear-phishing campaigns and building a backdoor.

During the course of researching the Winnti group, we came across previously unreported malware samples that we attributed to the group based on the malware arsenal and the use of registered domains as attack infrastructure. These samples led us to the discovery of additional C&C servers that provided us with more information than we initially expected.

A closer look at Hack520

Our initial investigation on the domains registered by Hack520 revealed that similar domains (listed below) were registered by another profile.

- hack520[.]co[.]kr
- shaiya[.]kr
- zhu[.]kr
- shenqi[.]kr
- zhuxian[.]kr

Several of these domains are linked to variants of malware that were used by the Winnti threat actor. Surprisingly enough, it does not take very long to get some information about Hack520: someone with this handle runs a blog and a Twitter account (with a handle close to Hack520) that is also directly linked to the blog.

Figure1_winnti

Figure 1: Twitter account of Hack520

One interesting detail about Hack520 is his apparent love for pigs, as seen in his use of the word in his email addresses. He also mentions his occupation as a "pig farmer" in online message boards. In addition, Hack520's tweets always show photos of the same animal, which is likely his pet pig.

The Twitter handle used by Hack520 indicates also an "est" portion. This "est" reference could refer to a hacking group with its own message board on which hack520 also posts regularly.

In one particular forum post, Hack520 mentions that he was previously jailed for a period of 10 months in a blog post dated May 31, 2009.

Figure2_winnti

Figure 2: Post from Hack520's blog

A rough translation of this message is as follows:

> "Fxxk, when I am released, the server is offline, I can't find the machine, the domain is expired, it is so bad. I wasted 10 months, I have failed and lost my money."

Hack520 seems to be very interested in hosting services and his profile fits that of a system administrator profile with some programming and hacking skills.

After further research, we were able to link Hack520 to different network administration activities, notably with a Virtual Private Server (VPS) hosting service. The way Hack520 signs his messages in one hacker forum provides a clue pointing to this connection. While one of his signatures uses his own blog domain, there is also a second signature which uses *93[.]gd*, a domain that was found to have been actively selling VPS services in the past. The email address *admin@93[.]gd* is linked to IP addresses owned by a certain user with the nickname "PIG GOD"—another reference to Hack520's passion for pigs.

Among the IP addresses owned by Hack520 is a whole/22 IP Range which we dubbed as the "PIG RANGE". The IP range for "PIG GOD" is *43[.]255[.]188.0/22*, which appears to be hosted in Hong Kong as seen in the information we found:

- inetnum: 43[.]255[.]188[.]0 - 43[.]255[.]191[.]255

- netname: PIG-HK
- description: PIG GOD
- country: HK
- admin-c: PG406-AP
- tech-c: PG406-AP
- person: pig god
- country: HK
- phone: +852-39437000
- e-mail: admin@66[.]to
- nic-hdl: PG406-AP
- mnt-by: MAINT-RAIBOW-HK
- changed: admin@66[.]to 20160917
- source: APNIC

The domain *66[.]to* leads to another website that shows Hack520's pet pig. It also reveals direct links to *secure[.]66[.]to* and *zhu[.]vn*, both of which also belong to Hack520 and contains his personal blog.

Figure3_winnti

Figure 3: Hack520's pet pig

We were able to find additional links between Hack520's "Pig network" and the Winnti group's activities. This includes hosting C&C domains that were used by Winnti such as mtrue.com, *shenqi[.]kr* and *zhu[.]kr*. We also found a live service selling VPS hosting at *secure[.]66[.]to*. The hosting services offered at *secure[.]66[.]to* are in fact hosting services rented to other companies worldwide. The contents found in *secure[.]66[.]to* often lead to *zhu[.]vn*, which is Hack520's domain for hosting his own private blog.

Figure4_winnti

Figure 4: Screenshot of secure[.]66[.]to

We found roughly 500 domain names that lead or have led to the "Pig network" between 2015 to March 2017. Most of these domains seem to have contained illegitimate content like pornography and online gambling. We highly suspect the "Pig network" to have also been used as a bulletproof hosting service for cybercriminals who are unrelated to the Winnti group. From what we've seen in Hack520's blog, as well as the infrastructure deployed around it, it is quite safe to say that Hack520 is involved in aspects of the VPS service activity provided to groups like Winnti and other cybercriminals or threat actors.

What we've learned

Threat actors like the Winnti group rarely ever stay static in terms of both tools and tactics. As we've already previously discussed in our 2017 predictions, these groups will constantly evolve and employ unique and advanced attack techniques. In addition, individuals like Hack520 prove that these threat actors are composed of varied individuals who have their own set of expertise. All of these things point to threat actors and groups like Winnti will continue to try different methods of attack.

Threat actors are always looking to expand the strategies they use, thus security practices and solutions that work for less organized cybercriminals might not work for determined groups who are willing to spend time, resources and manpower to accomplish their goals. As such, there is a need for everyone to be proactive when it comes to security, especially for organizations who are frequently the victims of targeted attacks. By creating awareness and using the right solutions, both individuals and organizations can take the steps needed to defend against the malicious tactics used by threat actors like the Winnti group.

APT & Targeted Attacks

We take a closer look at an individual who we believe might be connected to the Winnti group and provide better insights into some of the tools — notably the server infrastructures — as well as the scale in which they operate.

By: Trend Micro April 19, 2017 Read time: (words)

Content added to Folio