What even is Winnti?

risky.biz/whatiswinnti/

Op-Ed: It's time we had one last talk about Winnti...

By Daniel Gordon · July 20, 2020

Thanks largely to

inconsistent methodologies, poor clustering, and lack of collaboration, the word ‘Winnti’ has gradually been rendered meaningless.

We first heard the word ‘Winnti’ used to describe some specific attributes or actions: a malware family, stolen code signing certificates, rootkits, malware associated with suspected Chinese hacking, links to some specific Chinese personas (using hacker handles that spoke Chinese and claimed to live in China), and some specific targeting.

Seven years and a dozen studies later, we ended up with a name linked to at least 15 other names, some of which are likely to be separate groups. We’re at the point where Winnti doesn’t clearly represent any particular targeting, tools or techniques and also may not represent a group of people anymore.

It’s worth exploring how we got to this point to avoid repeating the same mistakes.

Origins

Winnti was named as a group in a 2013 blog by Kaspersky. The blog’s authors named the group based on a malware family previously named by Symantec. This very quickly brings us to lesson one: it’s not advisable to name a group exclusively based on the malware family, especially when the name was coined by another researcher.

Kaspersky’s research described intrusions going back to 2010, in which attackers targeted video game companies or used digital code signing certificates stolen from game companies.

Kaspersky listed some other notable characteristics in the campaigns it analysed, including unusual infrastructure DNS configurations, some relatively advanced rootkit malware, specific C2 choices and the use of characteristic Chinese malware such as PlugX.

Kaspersky discovered activity that generated revenue via creation of in-game currency or theft of source code, as well as targeting of specific ethnic groups that pointed to PRC sponsorship. Kaspersky researchers also picked up on some terrible OPSEC that revealed Chinese personas, further substantiated when some of the same handles showed up in a 2018 US Department of Justice indictment that pinned the theft of aerospace IP on the Jiangsu Province Ministry of State Security.

A year later FireEye published a report about how Chinese groups appeared to be sharing malware development, digital code signing certificates, and infrastructure. The company referenced some of the stolen digital certificates from Kaspersky's prior research but didn't at this stage name Winnti as a group.

By mid-2015, Kaspersky linked Winnti malware to other research on the Axiom Group (which may or may not be the same group). Axiom had been tied to a lot of intrusions, but most critically, its fingerprints were identified in the CCleaner, Netsarang, and ASUS software supply chain attacks. Kaspersky used similarities between malware used in these attacks and those previously attributed to 'Winnti' to illustrate that the latter was targeting a broader set of organisations than gaming companies. While these findings were important, attribution based on malware similarity alone is risky, especially when there is an existing body of research about malware being shared among different groups.

In 2016, Symantec published a blog about digital signing certificate abuse that is pertinent to the Winnti story. It referenced Kaspersky's earlier findings but didn't name it, describing it only as "a third party vendor". Here's another lesson: in any other field of research you would credit primary sources, even if you don't especially like them. It puts recognition where it's due, fosters collaboration and reduces the risk of "semantic drift" – where over time the definition of something loses connection to its original meaning.

To their credit, Symantec researchers tried to correct the course a little on their previous work - using the blog post to differentiate a group it referred to as Blackfly from the malware family Winnti. Unfortunately, Symantec's more cautious approach to naming conventions never caught on elsewhere.

Not content to let a chance pass by to participate in the Winnti goat rodeo, Cylance posted a blog in 2016 about PassCV activity ("PassCV" is a name coined by Blue Coat) and linked this activity to Winnti based on stolen code signing certificates. The post is light on malware analysis but mentions the use of several remote access trojans, ZXShell and Gh0st, in passing. Gh0st RAT has been used by multiple Chinese and North Korean groups. ZXShell

was a RAT commonly associated with Group72, which on the one hand also seems to correspond to Axiom/Winnti activity, but on the other, appears tied to APT27/Emissary Panda.

With the benefit of time on its side, Microsoft came up with the most sane approach, breaking down the groups using Winnti malware into BARIUM and LEAD. BARIUM targets "electronic gaming, multimedia, and internet content industries" as well as the occasional tech company, while LEAD is responsible for industrial espionage against manufacturing, pharmaceutical, engineering companies and academia. The tradecraft of the two groups could be distinguished at this point: BARIUM would attempt to establish rapport via social media and made use of malicious office macros, compiled HTML (.chm) files or shortcut (.lnk) files as first stages, while LEAD tended to just email the Winnti install package to victims or brute force credentials on a server and copy down the Winnti malware.

But in an April 2017 blog, Trend Micro bound the activity together again, describing "Winnti" as a criminal group that made fake antivirus engines in 2007 and shifted focus to hacking video game companies in 2009. Trend made these conclusions based on domain name registrations. This is another dangerous assumption.

ProtectWise' 401 Threat Research Group posted a couple of blogs about the "Winnti group"a few months later in July 2017, revealing the group's use of open source tools including Metasploit, BeEF, and Cobalt Strike. Both blogs were later updated to make clear that they were talking specifically about the LEAD group labeled by Microsoft. The 401TRG reports included some side-eye inducing conclusions. First, they included high confidence attribution to China. "High confidence" is usually reserved for governments that watch events happen over hacked closed circuit TVs - whereas these reports predated any indictments. Second, the researchers didn't provide a full explanation of how they were able to attribute activity to Winnti other than via stolen signing certificates. They did, on the positive side, show evidence of research - including a blog that summarises the public research various parties had done on the group so far.

In 2019, ESET attributed a software supply chain attack via Thai video games and a gaming platform to a group called "Winnti", as well as compromises of universities in Hong Kong. In a 2019 summary of all of this activity, ESET concluded that Axiom Group and "Winnti" are synonymous.

That same year – five years after its blog about supply chain overlap between Chinese groups – FireEye designated APT41 to be a China-based actor group responsible for a subset of "Winnti" activity. APT41 was described as a "dual espionage and cyber crime operation", conducting everything from espionage, targeting of activists, financially-motivated activity, and both the ASUS and Netsarang supply chain attacks. FireEye leaned on analysis of the operatives' working hours to speculate that it was a group of state-sponsored contractors that also do side-gigs to make more money. FireEye bundled in to that designation previous activity it identified under the name GREF and the use of stolen digital

signing certificates, and mentioned that APT41 shared malware with seven other suspected Chinese groups, including China Chopper and Sogu. It didn't link it to APT27/Emissary Panda activity.

In 2020, Cylance, now owned by Blackberry, updated the public on its view – describing activity that used a Linux rootkit and shared links to Android malware.This time around the Cylance analysis put more effort into differentiating activity based on targeting, while acknowledging the malware was being shared between various groups.

This year, FireEye also published a blog concluding that APT41 went after many different kinds of victims using Citrix, Cisco and Zoho ManageEngine vulnerabilities. It again mentioned the use of open source tools and living off the land techniques such as Metasploit, BITSjobs, and Cobalt Strike.

We continue to see the name 'Winnti' routinely mentioned in numerous news reports. But what even is Winnti at this point?

What have we learned from "Winnti"?

The name 'Winnti' has been diluted to the point where it's no longer useful. I understand the benefits of using threat intelligence reporting as a form of marketing, but it's still research, and should be treated accordingly.

When relating activity to an existing group, talk to the originator about their understanding to avoid hijacking the name.

When your cluster diverges from the originator's, use your own group name and explain how and why it diverges. Great reports often express confidence levels, talk about why links are significant, and show how different data can lead to different analysis. Using your own group name can also help keep other researchers from dumping their analysis, good or bad, into your activity bucket without you having a say in the matter. We should prioritise the quality of our research over the clicks and hype from using a recognisable group name.

Don't be afraid to make updates to published research or retract them under extreme circumstances. It's better to have integrity and temporary embarrassment than have your organisation's name be associated with bad attribution for eternity.

I've made all the mistakes. And I've learned from them. Admitting to and learning from mistakes is part of the journey to good analysis. Sometimes good research requires asking other researchers for explanations or collaborating.

Researchers should lean on better-defined actor names like LEAD and BARIUM or stick to names of their own devising to avoid creating more confusion. And in case I've left any room for doubt about what we should do with the name 'Winnti', here's my suggestion.

Daniel Gordon is a CTI analyst in the defence sector.