Report on Winnti Group

Overview

The Winnti group, also known as Winnti Group and Blackfly, is an intrusion-set that primarily engages in information theft and espionage, with financial crime being another motivation. The group is believed to have Chinese origins and has been active since at least 2010. While the gaming industry has been heavily targeted, the group has expanded its scope of targeting. Reports suggest that the Winnti Group is closely linked to other threat groups, including Axiom, APT17, and Ke3chang. The group was first observed on May 31, 2017, and the last known activity was on April 15, 2022.

Stats

The set is related to these malwares:
- 3 backdoors (PipeMon, Winnti and PlugX)
- 2 info stealers (Winnti and PlugX)
- 2 exfiltrations (Winnti and PlugX)
- 2 reconnaissances (Winnti and PlugX)
- 1 downloader (Winnti)
- 1 tunneling (Winnti)
- 1 rootkit (Winnti)
- 1 keylogger (PlugX)

Winnti group is related to these tools:
- 1 tunneling (Cobalt Strike)
- 1 exfiltration (Cobalt Strike)
- 1 loader (Cobalt Strike)
- 1 backdoor (Cobalt Strike)
- 1 vulnerability scanner (Cobalt Strike)
- 1 keylogger (Cobalt Strike)

It is related to these attack-patterns:
- 1 resource-development (T1583.001 - Domains)
- 1 command-and-control (T1105 - Ingress Tool Transfer)
- 2 discoveries (T1057 - Process Discovery and T1083 - File and Directory Discovery)
- 2 defense-evasions (T1553.002 - Code Signing and T1014 - Rootkit)

Relationships

Winnti Group

To clarify, the Winnti group has targeted entities in the defense and financial sectors, with locations including Thailand, South Korea, Peru, Brazil, the United States, the Philippines, Japan, Indonesia, China, and Vietnam. The group is believed to be based in China and employs the malware PlugX and the tool Cobalt Strike, using the attack pattern T1014 - Rootkit.

Cobalt Strike

Cobalt Strike has been used not only by the ToddyCat Campaign in June 2022 but also by numerous other intrusion-sets, such as LuminousMoth, Bronze Highland, FIN12, PassCV, Pinchy Spider, Gold Southfield, TA2101, Maze Team, Mustang Panda, Bronze President, Sprite Spider, Gold Dupont, TA511, MuddyWater, Rancor, Winnti Group, UNC2447, Barium, ChamelGang, Harvester, Earth Wendigo, TAG-28, OldGremlin, Karakurt, SaintBear, Lorec53, TAG-22, Aquatic Panda, APT 41, DarkHydrus, FIN7, Lead, APT37, menuPass, Earth Lusca, Indrik Spider, APT19, Mustang Panda, ALTDOS, APT32, Cobalt Group, Chimera, Doppel Spider and Operation Ghostwriter.

Mitre Matrix

Source	Name	Tactic	ATT&CK Code	Description
Winnti Group	T1014 - Rootkit	defense-evasion		Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits) Rootkits or rootkit enabling

				functionality may reside at the user or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or [System Firmware](https://attack.mitre.org/techniques/T1542/001). (Citation: Wikipedia Rootkit) Rootkits have been seen for Windows, Linux, and Mac OS X systems. (Citation: CrowdStrike Linux Rootkit) (Citation: BlackHat Mac OSX Rootkit)

IOCs

Source	Type	Value
Winnti Group	ipv4-addr	60.186.72.92
Cobalt Strike	domain-name	unit42.paloaltonetworks.com

Useful Resources

Useful material to know better Winnti Group can be found at: https://attack.mitre.org/groups/G0044, http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates, https://401trg.github.io/pages/burning-umbrella.html, https://securelist.com/winnti-more-than-just-a-game/37029/, http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf and https://securelist.com/games-are-over/70991/.