Report on Winnti Group

Overview

Winnti group is an intrusion-set, which operates also under the name of Winnti Group and Blackfly. The primary motivation of the group is information theft and espionage, followed by information theft and espionage and financial crime. It was observed for the first time on 31 May 2017 and for the last time on 15 April 2022. The description of the group is: [Winnti Group] is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting. Some reporting suggests a number of other groups, including [Axiom], [APT17], and [Ke3chang], are closely linked to [Winnti Group].

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

The set targets these identities [Unknown Defense] and [Unknown Financial] and these locations Thailand, Korea, Republic of, South Korea, Peru, Thailand, Brazil, USA, Philippines, Japan, Indonesia, CN and Vietnam. It appears to be located in CN. Winnti group uses this malware PlugX and this tool Cobalt Strike. It uses this attack-pattern T1014 - Rootkit.

Cobalt Strike

Cobalt strike is used by this campaign ToddyCat Campaign June 2022 and these intrusion-sets 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/.