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].

Relationships

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

Stats

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

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

It is related to these attack-patterns:

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

Mitre Matrix

Name	Tactic	ATT&CK Code	Description
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

Type	Value
ipv4-addr	60.186.72.92

Useful Resources

Useful material to know better the set 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/.

Report on Cobalt Strike

Overview

Cobalt strike is a tool. The description of Cobalt Strike is: Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named 'Beacon' on the victim machine. Beacon includes a wealth of functionality to the attacker, including, but not limited to command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning and lateral movement. Beacon is in-memory/file-less, in that it consists of stageless or multi-stage shellcode that once loaded by exploiting a vulnerability or executing a shellcode loader, will reflectively load itself into the memory of a process without touching the disk. It supports C2 and staging over HTTP, HTTPS, DNS, SMB named pipes as well as forward and reverse TCP; Beacons can be daisy-chained. Cobalt Strike comes with a toolkit for developing shellcode loaders, called Artifact Kit.

The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable. Cobalt strike types are backdoor, vulnerability scanner, keylogger, tunneling, loader and exfiltration.

Relationships

The tool is used by this campaign ToddyCat Campaign June 2022 and these intrusion-sets APT32, Chimera, Cobalt Group, Doppel Spider, Bronze Highland, Operation Ghostwriter, Indrik Spider, Earth Lusca, PassCV, APT19, Pinchy Spider, Gold Southfield, Mustang Panda, ALTDOS, DarkHydrus, TA511, APT37, FIN7, Lead, Aquatic Panda, APT 41, menuPass, TAG-

22, OldGremlin, Karakurt, SaintBear, Lorec53, Winnti Group, Barium, UNC2447, ChamelGang, TAG-28, Earth Wendigo, Harvester, Mustang Panda, Bronze President, Sprite Spider, Gold Dupont, Rancor, MuddyWater, LuminousMoth, FIN12 and TA2101, Maze Team.

IOCs

Type	Value
domain-name	unit42.paloaltonetworks.com

Useful Resources

Useful material to know better Cobalt Strike can be found at: https://www.cobaltstrike.com/, https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html, https://blogs.jpcert.or.jp/en/2018/08/volatility-plugin-for-detecting-cobalt-strike-beacon.html, https://github.com/JPCERTCC/aa-tools/blob/master/cobaltstrikescan.py, https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html, http://blog.morphisec.com/new-global-attack-on-point-of-sale-systems, https://www.lac.co.jp/lacwatch/people/20180521_001638.html, https://www.pentestpartners.com/security-blog/cobalt-strike-walkthrough-for-red-teamers/, https://www.bleepingcomputer.com/news/security/threat-actors-use-older-cobalt-strike-versions-to-blend-in/, https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf, https://blog.talosintelligence.com/2020/09/coverage-strikes-back-cobalt-strike-paper.html, https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/, https://www.darkreading.com/threat-intelligence/how-to-identify-cobalt-strike-on-your-network/a/d-id/1339357, https://www.deepinstinct.com/2021/03/18/cobalt-strike-post-exploitation-attackers-toolkit/, https://www.darkreading.com/attacks-breaches/cobalt-strike-becomes-a-preferred-hacking-tool-by-cybercrime-apt-groups/d/d-id/1341073, http://www.intel471.com/blog/cobalt-strike-cybercriminals-trickbot-qbot-hancitor, https://blog.malwarebytes.com/researchers-corner/2021/06/cobalt-strike-a-penetration-testing-tool-popular-among-criminals/, https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware, https://labs.sentinelone.com/hotcobalt-new-cobalt-strike-dos-vulnerability-that-lets-you-halt-operations/, https://www.intezer.com/blog/malware-analysis/cobalt-strike-detect-this-persistent-threat/, https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/, https://www.recordedfuture.com/detect-cobalt-strike-inside-look/, https://elis531989.medium.com/the-squirrel-strikes-back-analysis-of-the-newly-emerged-cobalt-strike-loader-squirrelwaffle-937b73dbd9f9, https://blog.nviso.eu/2021/10/21/cobalt-strike-using-known-private-keys-to-decrypttraffic-part-1/, https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot, https://asec.ahnlab.com/en/31811/, https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2-profile/, https://attack.mitre.org/software/S0154/, https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike and https://otx.alienvault.com/browse/pulses?q=tag:Cobalt%20Strike.