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.

Relationships

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.

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 powerful tool used for penetration testing, which allows attackers to deploy an agent called 'Beacon' on a victim's machine. This agent provides the attacker with a range of functionalities, such as command execution, keylogging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning, and lateral movement. Beacon is designed to be in-memory and file-less, meaning it consists of stageless or multi-stage shellcode that can be loaded into the memory of a process without writing to the disk, making it difficult to detect. Cobalt Strike supports various communication methods, including HTTP, HTTPS, DNS, SMB named pipes, and TCP, and can be daisy-chained. The tool also comes with Artifact Kit, a toolkit for developing shellcode loaders. The Beacon implant is popular among targeted attackers and criminal users due to its stability, well-written code, and high level of customization. Cobalt Strike can be used for various purposes, including backdoor creation, vulnerability scanning, keylogging, tunneling, loader creation, and exfiltration.

Relationships

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.

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.