Overview of Winnti Group intrusion set.

The set has been publicly released on October 10, 2022. The intrusion set's aliases are “Winnti Group” and “Blackfly”. The set's description 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].

The intrusion set has been first observed on May 31, 2017. It has been last seen on Aprle 15, 2022. The intrusion set's resource level estimation is not provided.

Motivation.

Its primary motivation is information theft and espionage. The set's secondary motivation is information theft and espionage and financial crime. Its goal is not provided.

Associated campaigns.

No entities found.

Associated victims.

[Unknown Financial].

[Unknown Financial] has been published on October 20, 2021. Its identity class is not provided. Its sector is media. The identity's description is not provided.

[Unknown Defense].

[Unknown Defense] has been released on October 20, 2021. Its identity class is not provided. The identity's sector is defense. Its description is not provided.

Associated MITRE ATT&CK TTPs.

T1014 - Rootkit

T1014 - Rootkit name is "T1014 - Rootkit". The attack pattern's description is

> 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. 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]. Rootkits have been seen for Windows, Linux, and Mac OS X systems.

Overview of Cobalt Strike.

The tool has been published on December 10, 2020. Its description 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.