← BACK

Operation SMN – Winnti Update

n the cyber security industry to target the malware used extensively by the threat actor group Axiom. During our investigations of active Axiom compromises, we came across new versions of the Winnti malware, which differed from previously observed versions that targeted online gaming companies to steal source code and digital certificates[1]. Digital certificates stolen by Winnti operators have later been used in other identified attacks[2].

Based on the compromises we were able to observe, we believe with high confidence that the Winnti operators were not the same actors as those who initially installed and leveraged Hikit in that environment. Instead, these operators made use of Hikit to gain access to the environment and then move laterally within that network to install Winnti as part of their own individual unique tool set. These operators also leveraged a completely different set of techniques, tactics, and procedures (TTPs) than were previously observed by Hikit operators, which served to further differentiate them from the previous group of actors.

Winnti was first reported by Kaspersky researchers in 2013. New versions of Winnti that we observed and captured, compiled from mid to late 2014, appear to have added extensive anti - analysis components but largely retain the same core functions as previous versions. Given the changes in Winnti samples, Novetta is releasing an in depth reverse engineering report providing an analysis of the startup sequence of Winnti, a basic overview of the malware, and information on the command and control (C2) communication protocol used by the samples we captured. This report will give defenders insight into the newer Winnti threat in addition to providing valuable knowledge to better detect and remediate the Winnti threat within a defender’ s infrastructure. We have also included a list of hashes for samples that can be found in VT, as well as yara signatures that can be used by incident responders or security teams to identify samples.

NOVETTA

WINNTI
ANALYSIS

As part of Operation SMN, Novetta analyzed recent versions of the Winnti malware. The samples, compiled from mid- to late 2014, exhibited minimal functional changes over the previous generations Kaspersky reported in 2013.[1] What is of note, however, is the increased scrutiny found within the Winnti dropper component that attempts to frustrate analysis of the malware.

Based on multiple active compromises by the Axiom threat group, Novetta was able to capture and analyze new Winnti malware samples. It should be noted that operators of Winnti that were observed by Novetta leveraged existing Axiom-specific malware infections (Hikit) to move laterally and install Winnti in the furtherance of their objectives. It is with high confidence that we assess the operators of Winnti in these monitored environments were not the same actors who originally installed and leveraged Hikit.

This report will focus on three different aspects of the Winnti malware: the start-up sequence of Winnti from the initial infection to steady state, the basics of the Winnti malware, and the command and control (C2) communication protocol.

FROM INSTALLATION TO EXECUTION
The installation process of Winnti by means of the dropper has changed very little since the Winnti version 1.1 (as defined by Kaspersky) droppers of July 2012. The samples Novetta obtained from the active Axiom infection were compiled in mid- to late 2014 and represent what Novetta is referring to as version 3.0 of the Winnti lineage (in order to prevent muddying the versioning scheme Kaspersky has already established).

There are four distinct components within the Winnti malware's installation to execution cycle: a dropper, a service, an engine, and a worker. The installation that Novetta observed of Winnti on a victim's machine requires multiple steps and depends on the dropper, service, and the loader component in order to accomplish the steps. After a successful infection, the activation of Winnti on a victim's machine requires multiple steps as well as coordination between the service, engine, and worker components. The complexity of the installation and activation processes is significant and more involved than typical malware installation and activation procedures. This additional complexity ultimately does not seem to serve a significant purpose other than to perhaps frustrate analysis by defenders.

[1] Kaspersky. "Winnti: More than just a game". http://kasperskycontenthub.com/wp- content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf. 10 April 2014.

1

Detection information:

Download the Winnti Analysis report here (pdf)

Yara Signatures for Winnti family (txt)

List of sha256 hashes for some of the Winnti samples found in VirusTotal (txt)

1 Securelist. “Winnti FAQ. More than just a game” . April 2013.

2 FireEye. “Supply Chain Analysis: From Quartermaster to Sunshop” . August 2014.

Read more about the author:
Novetta Threat Research Group

Category: Novetta Nexus / Novetta Threat Research Group
Tag(s): Axiom / Hikit / Operation SMN / Sup / TTPs

CATEGORIES ›

SUBSCRIBE TO OUR BLOG

Name *

First Last

Email *

Topics *

□ Advanced Analytics

□ Big Data and Entity Analytics

□ Cyber Security

□ Threat Research Group

Submit

Webinars Podcasts

Infographics

Novetta Entity Analytics Webinar: 3 Ways to Make Sure Potential Fraudsters Have Nowhere to Hide

Novetta Entity Analytics Webinar: 4 Signs You Need an Advanced Customer 360

Novetta Entity Analytics Webinar: 5 Key Factors to Optimizing Your Big Data and Advanced Analytics

Novetta Entity Analytics Webinar: Reach the Cloud with Big Data and Advanced Analytics

CONTRIBUTORS

Bios

CONTACT US

We’ d be happy to prove to you just how effective our products and solutions can be.

REQUEST MORE INFO

NOVETTA

7921 Jones Branch Drive, McLean, VA 22102 (571) 282-3000