

[NEWS & EVENTS](#)[CONTACT](#)

NOVETTA NEXUS

[← BACK](#)

Operation SMN – Winnti Update



NOVETTA
PRODUCTS
From Complexity to Clarity

[SOLUTIONS](#)[ABOUT](#)[RESOURCES](#)[CAREERS](#)[BLOG](#)

...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 certificates¹. Digital certificates stolen by Winnti operators have later been used in other identified attacks².

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.

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.

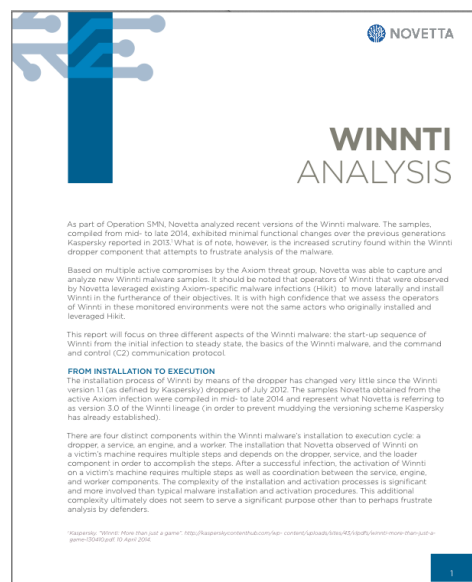
Read more about the author:

□

[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 *

FirstLast

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

© 2015 Novetta Website | [Terms and Conditions](#) | Responsive WordPress Website by [HyperArts](#)

