ultraviolet

THREAT REPORT:

Zloader: Back in Action (But Quietly)

Services Performed By:
UltraViolet Cyber
Meredith Glass
(443) 351-7630
info@uvcyber.com

Published Date:
8 May 2024

Contents

1 Executive Summary

The Zloader malware is a trojan derived from the Zeus banking trojan that originally targeted German banks in 2015-2016. The code and capabilities of the trojan evolved, and it started to be marketed as “Silent Night” in underground forums around 2019, following trends similar to other MaaS, complete with a clever and catchy name, moved from fraud to ransomware to a fully sophisticated modular trojan. The current iteration of Zloader offers anti-analysis features, natively supported 64-bit Windows loader and encrypted network communications to its C2 server.

2 Technical Analysis

To avoid analysis and to decrease the efficacy of sandboxing techniques, Zloader utilizes junk code, resolves the majority of its imports at runtime and has explicit expectations for the filename, wherein failure to match the expected filename causes execution to stop. Since malware sandboxes will rename files, this can be problematic for analysis utilizing sandboxes.

ZeuS fits into this with its overlay section called ‘PeSettings’ where installation information is stored. If a system is not already infected, the trojan will recognize this and follow through with generating the information needed to install and uniquely identify the RC4 key for the host. The PeSettings will be re-encrypted and overlay data overwritten modifying the header and data size.

For C2 communications, if the primary server is unavailable, Zloader utilizes DGA which is a fairly common tactic in a number of malware families and their associated campaigns.

Zloader’s static configuration is encrypted using the RC4 stream cipher and ThreatLabZ observed the same RSA public key for each of the unique samples analyzed.

Once Zloader has been installed on a system, access to the infected systems can be sold to affiliates and additional malicious activities can be achieved including ransomware and installation/misuse of legitimate tools (e.g., Cobalt Strike).

The Zloader trojan typically arrives via malicious Office or Google documents containing malicious macros sent by email or through a malicious advertisement delivery mechanism. This is achieved by compromise of legitimate domains and adding malicious subdomains impersonating the legitimate domain/service. Attempting to download a product from the compromised domain being impersonated results in redirection to the threat actor’s domain. According to Microsoft, the Zloader operators have typically used the *REG.RU, LLC* registrar and the *.site* TLD.

© 2023 ULTRAVIOLET. ALL RIGHTS RESERVED.

Following are some of the collected artifacts amongst various sources accessed throughout this analysis:

SHA256 IOCs from Zloader samples:
cba9578875a3e222d502bb6a85898939bb9e8e247d30fcc0d44d83a64919f448
85962530c71cd31c102853d64a8829f93b63bd1406bdec537b9d8c200f8f0bcc
b1a6bf93d4ee659db03e51a3765d4d3c2ee3f1b56bd9b701ab5939d63f57d9ee
85b1a980eb8ced59f87cb5dd7702e15d6ca38441c4848698d140ffd37d2b55e6
038487af6226adef21a29f3d31baf3c809140fcb408191da8bc457b6721e3a55
16af920dd49010cf297b03a732749bb99cc34996f090cb1e4f16285f5b69ee7d
25c8f98b79cf0bfc00221a33d714fac51490d840d13ab9ba4f6751a58d55c78d
2cdb78330f90b9fb20b8fb1ef9179e2d9edfbbd144d522f541083b08f84cc456
83deff18d50843ee70ca9bfa8d473521fd6af885a6c925b56f63391aad3ee0f3
98dccaaa3d1efd240d201446373c6de09c06781c5c71d0f01f86b7192ec42eb2
adbd0c7096a7373be82dd03df1aae61cb39e0a155c00bbb9c67abc01d48718aa
b206695fb128857012fe280555a32bd389502a1b47c8974f4b405ab19921ac93
b47e4b62b956730815518c691fcd16c48d352fca14c711a8403308de9b7c1378
d92286543a9e04b70525b72885e2983381c6f3c68c5fc64ec1e9695567fb090d
eb4b412b4fc58ce2f134cac7ec30bd5694a3093939d129935fe5c65f27ce9499
f03b9dce7b701d874ba95293c9274782fceb85d55b276fd28a67b9e419114fdb
f6d8306522f26544cd8f73c649e03cce0268466be27fe6cc45c67cc1a4bdc1b8
fa4b2019d7bf5560b88ae9ab3b3deb96162037c2ed8b9e17ea008b0c97611616
fbd60fffb5d161e051daa3e7d65c0ad5f589687e92e43329c5c4c950f58fbb75

Zloader C2 URLs:
hxxps[://]adslstickerhi[.]world
hxxps[://]adslstickerni[.]world
hxxps[://]dem.businessdeep[.]com

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber is actively threat hunting for IOCs and artifacts related to emerging threats
- Monitoring hosts for potential compromise or unusual activity based on up-to-date alerting, signatures, and rules
- Communicating with customers promptly when vulnerabilities that may be exploited are shown to be present either via threat hunting or in information gathered during normal workflow

4 What Customers Can Do

- Proceed to only utilize approved browsers with appropriate security controls in place and avoid downloading applications from the web or documents from email attachments that aren't thoroughly vetted from a known source
- Avoid activity involving the disabling or compromise of AV or installed detection software on company workstations

© 2023 ULTRAVIOLET. ALL RIGHTS RESERVED.

5 References

Any.run:

Title: “Zloader”
Source: Any.run. Retrieved from any.run/malware-trends/zloader

Title: “Loader Now Targets 64-bit Systems: Analyze The New Version in ANY.RUN”
Source: Any.run. Retrieved from any.run/cybersecurity-blog/new- zloader-campaign/

Thehackernews.com:

Title: “Loader Malware Evolves with Anti-Analysis Trick from Zeus Banking Trojan”
Source: The Hacker News. Retrieved from thehackernews.com/2024/05/zloader-malware-evolves-with-anti.html

Microsoft:

Title: “Dismantling ZLoader: How malicious ads led to disabled security tools and ransomware”
Source: Microsoft. Retrieved from www.microsoft.com/en-us/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/

SC Magazine:

Title: “Increased stealth introduced in updated Zloader malware”
Source: SC Media. Retrieved from www.scmagazine.com/brief/increased-stealth-introduced-in-updated-zloader-malware

Zscaler :

Title: “Zloader Learns Old Tricks”
Source: Zscaler ThreatLabz. Retrieved from www.zscaler.com/blogs/security-research/zloader-learns-old-tricks

Title: “loader: No Longer Silent in the Night”
Source: Zscaler ThreatLabz. Retrieved from www.zscaler.com/blogs/security-research/zloader-no-longer-silent-night

© 2023 ULTRAVIOLET. ALL RIGHTS RESERVED.