Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

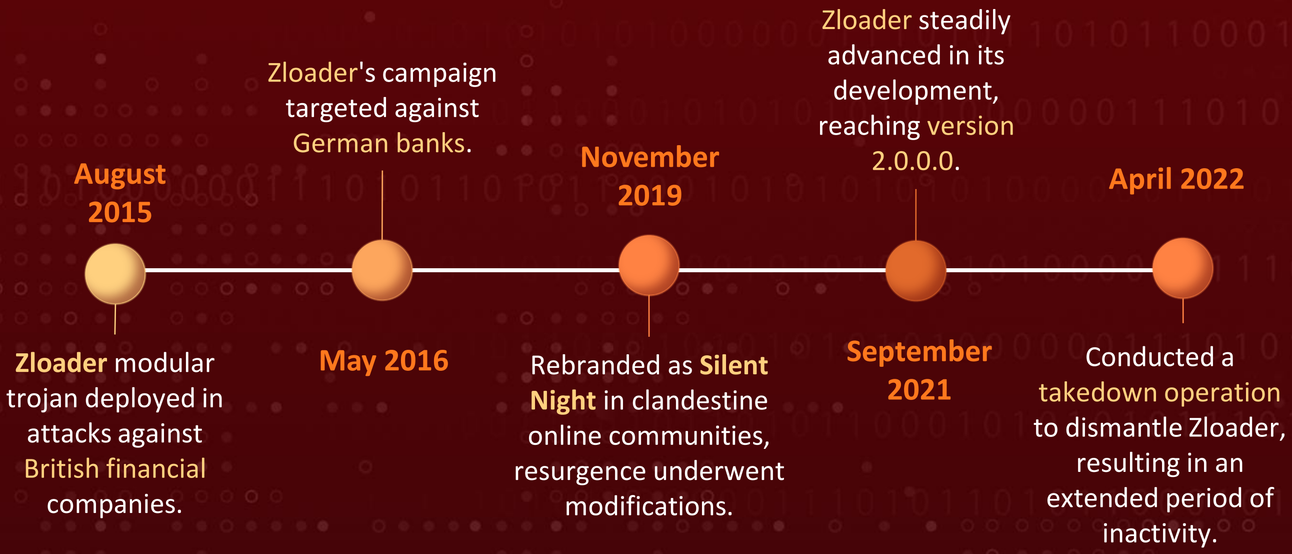
ZLoader's Resurgence after Two Years in the Shadows

Date of Publication	Admiralty Code	TA Number
January 22, 2024	A1	TA2024026

Summary

Attack Commenced: September 2023
Malware: Zloader (aka Terdot, DELoader, or Silent Night)
Attack Region: Worldwide
Attack: Zloader is a highly sophisticated Trojan originating from the leaked Zeus source code. Notable for its adaptive nature, the malware continuously evolved through each campaign since its debut in August 2015. After nearly two years of dormancy, Zloader reemerged with new iterations.

Attack Timeline



August 2015
Zloader modular trojan deployed in attacks against British financial companies.

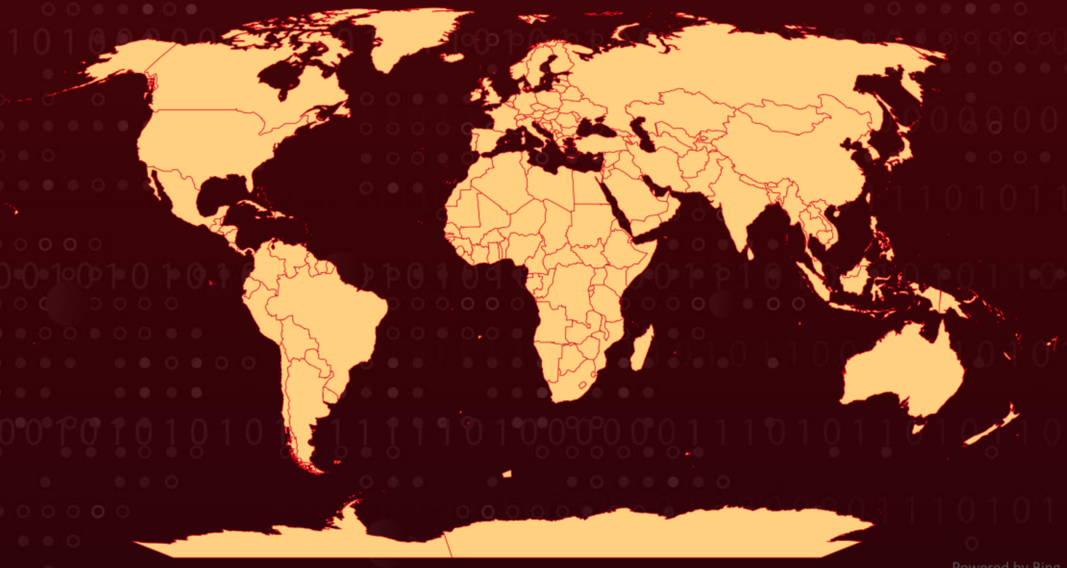
May 2016
Zloader's campaign targeted against German banks.

November 2019
Rebranded as **Silent Night** in clandestine online communities, resurgence underwent modifications.

September 2021
Zloader steadily advanced in its development, reaching version 2.0.0.0.

April 2022
Conducted a takedown operation to dismantle Zloader, resulting in an extended period of inactivity.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 Zloader, also known as Terdot, DELoader, or Silent Night, is a sophisticated Trojan derived from the leaked Zeus source code. This modular malware stands out for its adaptive nature, constantly evolving and undergoing transformations with each campaign, showcasing significant development since its initial release in August 2015.

#2 ZLoader has maintained prominence among attackers due to its incorporation of defense evasion mechanisms, such as the ability to disable security measures and antivirus tools. Additionally, it offers access-as-a-service to affiliate groups, including those involved in ransomware operations. After a pause of nearly two years, Zloader resurfaced with a fresh iteration that began development in September 2023.

#3 Versions 2.1.6.0 and 2.1.7.0 of Zloader introduced tangible enhancements to the loader module, featuring the integration of RSA encryption, updates to the domain generation algorithm, and compilation for 64-bit Windows operating systems for the first time.

#4 The latest Zloader samples employ advanced obfuscation techniques, including custom obfuscation, API import hashing, incorporation of junk code, filename checks, and string obfuscation. Zloader continues to rely on HTTP POST requests for communication with its command-and-control (C2) server. Having posed a significant threat for an extended period, the resurgence of Zloader raises concerns about potential new ransomware attacks in the foreseeable future.

Recommendations

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Enhance Endpoint Security: Strengthen endpoint security by employing measures such as endpoint detection and response (EDR) solutions. These tools can help identify and respond to suspicious activities associated with ZLoader.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	TA0010 Exfiltration	T1059 Command and Scripting Interpreter	T1059.006 Python
T1574 Hijack Execution Flow	T1211 Exploitation for Defense Evasion	T1543 Create or Modify System Process	T1068 Exploitation for Privilege Escalation
T1046 Network Service Discovery	T1057 Process Discovery	T1027 Obfuscated Files or Information	T1105 Ingress Tool Transfer
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	038487af6226adef21a29f3d31baf3c809140fcb408191da8bc457b6721e3a55, 16af920dd49010cf297b03a732749bb99cc34996f090cb1e4f16285f5b69ee7d, 25c8f98b79cf0bfc00221a33d714fac51490d840d13ab9ba4f6751a58d55c78d, 2cdb78330f90b9fb20b8fb1ef9179e2d9edfbbd144d522f541083b08f84cc456, 83deff18d50843ee70ca9bfa8d473521fd6af885a6c925b56f63391aad3ee0f3, 98dccaaa3d1efd240d201446373c6de09c06781c5c71d0f01f86b7192ec42eb2, adbd0c7096a7373be82dd03df1aae61cb39e0a155c00bbb9c67abc01d48718aa, b206695fb128857012fe280555a32bd389502a1b47c8974f4b405ab19921ac93,

TYPE	VALUE
SHA256	b47e4b62b956730815518c691fcd16c48d352fca14c711a8403308de9b7c1378, d92286543a9e04b70525b72885e2983381c6f3c68c5fc64ec1e9695567fb090d, eb4b412b4fc58ce2f134cac7ec30bd5694a3093939d129935fe5c65f27ce9499, f03b9dce7b701d874ba95293c9274782fceb85d55b276fd28a67b9e419114fdb, f6d8306522f26544cd8f73c649e03cce0268466be27fe6cc45c67cc1a4bdc1b8, fa4b2019d7bf5560b88ae9ab3b3deb96162037c2ed8b9e17ea008b0c97611616, Fbd60fffb5d161e051daa3e7d65c0ad5f589687e92e43329c5c4c950f58fbb75
URLs	hxxps://adslstickerhi[.]world, hxxps://adslstickerni[.]world, hxxps://dem.businessdeep[.]com

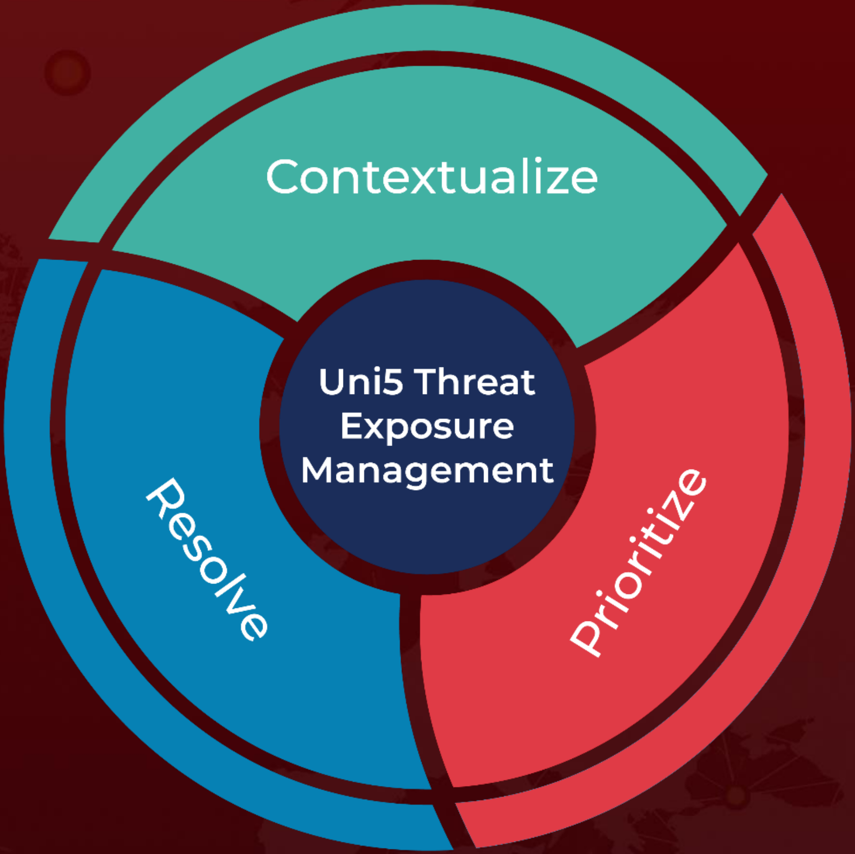
References

https://www.zscaler.com/blogs/security-research/zloader-no-longer-silent-night

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 22, 2024 • 3:30 AM

More at www.hivepro.com