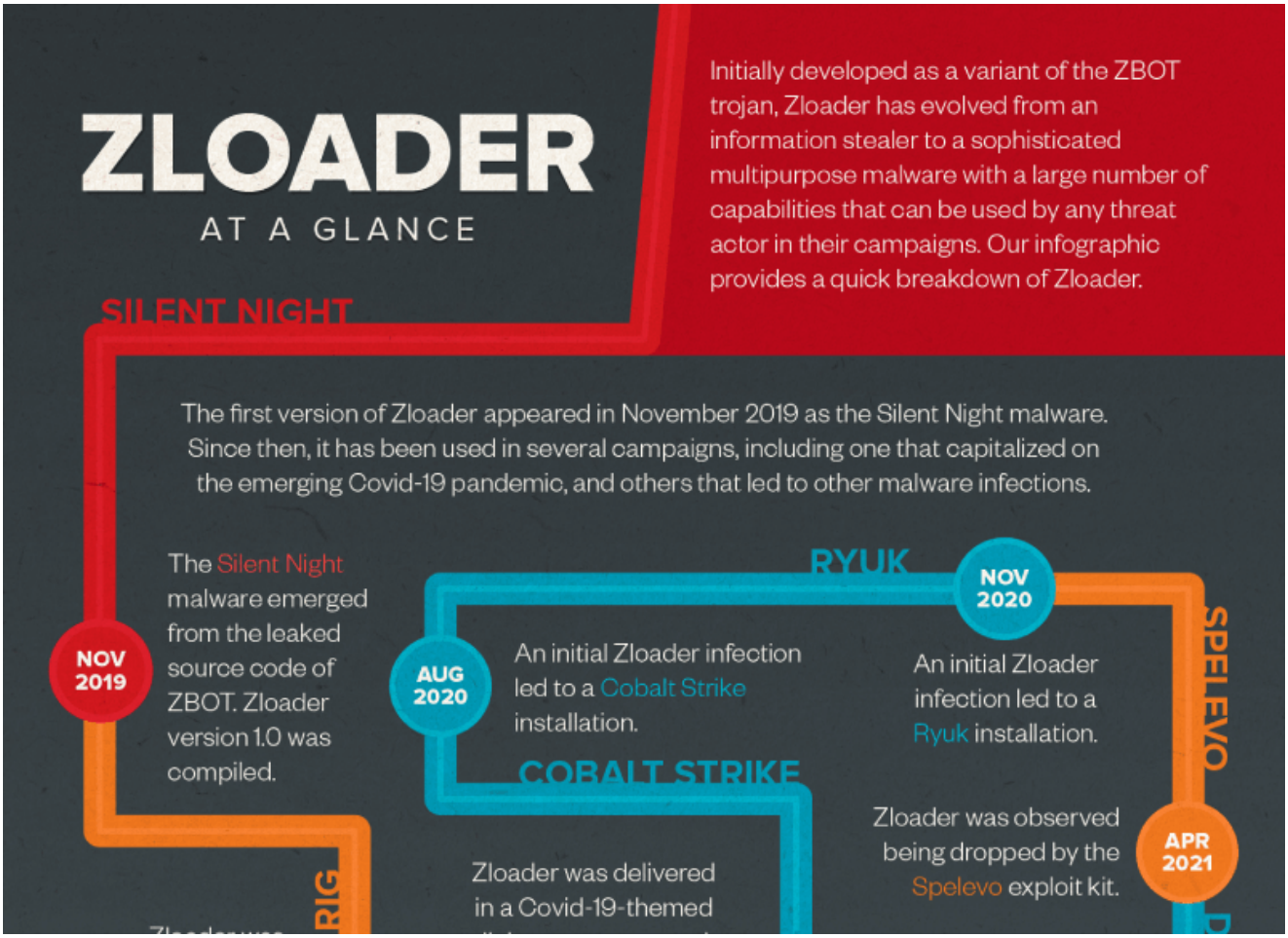
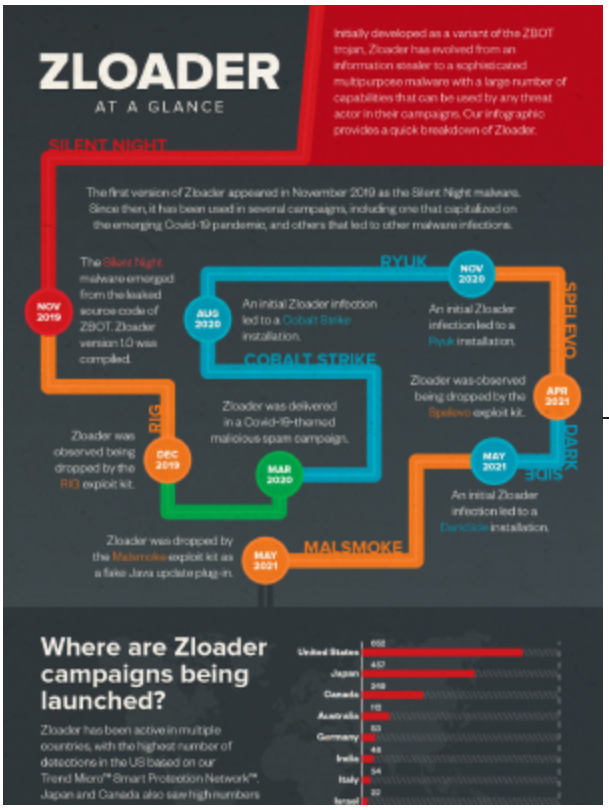
Zloader Campaigns at a Glance

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/zloader-campaigns-at-a-glance





View infographic: Zloader Campaigns at a Glance

The ZBOT (aka Zeus) trojan has been one of the most prolific and enduring malware families of the past 20 years. After its first appearance in 2006, its source code was leaked in 2011, leading to a plethora of new variants that plagued organizations over the succeeding years.

One of the most notable recent ZBOT variants is Zloader. First compiled under the name Silent Night in late 2019, it has evolved from being an information stealer to a multipurpose dropper that provides malicious actors the means to install and execute other malware and tools such as Cobalt Strike, DarkSide, and Ryuk. In addition, it has other capabilities, such as the ability to provide remote access to attackers and install plug-ins for additional routines.

Zloader has multiple delivery methods, such as via email campaigns or downloads by other malware and hacking tools. One of the most basic yet reliable methods for individuals and organizations to avoid being infected by Zloader and other malware with similar arrival techniques is to apply security best practices to their emails. This includes avoiding downloading attachments or selecting links from emails that look suspicious or appear to be out of context.

Zloader's versatility has made it a popular and effective campaign tool for any threat actor that is willing to pay for it. We already witnessed this in past campaigns — some of which took advantage of current events such as the Covid-19 pandemic — and we can expect to see it again in future campaigns from other threat actors.

Organizations can mitigate the impact of Zloader by employing robust security solutions and services. Trend Micro's robust native XDR capabilities are tied together by Trend Micro Vision One™, which connects email, endpoints, servers, cloud workloads, and networks in

order to provide a better context and perspective of the entire chain of events of an attack, while also allowing security personnel to investigate and act from a single place.

Furthermore, managed security services, such as Trend Micro™ Managed XDR, provides expert threat monitoring, correlation, and analysis from experienced cybersecurity professionals via a single and capable source of detection, analysis, and response. This expertise is further bolstered by AI-optimized, Trend Micro solutions that draw from global threat intelligence.

MITRE ATT&CK techniques

Zloader uses the following tactics and techniques, as mapped out according to the MITRE ATT&CK Matrix.

Tactic	MITRE ID and Technique	Details
Initial Access	T1189 - Drive-by Compromise	Zloader can be downloaded through drive-by compromise via Malsmoke, RIG Exploit Kit, and Spelevo
	T1566 - Phishing	Zloader can arrive via phishing emails with attached XLS downloader files
Execution	T1204 - User Execution	User can execute the XLS Zloader downloader file manually

T1064 - Scripting	Zloader can be downloaded by VBS or Javascripts	
T1059 - Command and Scripting Interpreter		
T1106 - Native API	Zloader hooks native API from user32.dll and ntdll.dll to redirect execution to Zloader DLL	
Persistence	T1060 - Registry Run Keys/Startup Folder	Creates persistence using the following registry: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
T1547- Boot or Logon Autostart Execution		
Privilege Escalation	T1055 - Process Injection	Zloader injects its loader or core component to msiexec.exe

Defense Evasion	T1027 - Obfuscated files or information	Instead of presenting arithmetic functions in a standardized manner and directly hardcoding constants, Zloader tries to confuse the analyst by obfuscating these in a form of various, dedicated functions
T1140 – Deobfuscate/ Decode Files or Information	Zloader performs XOR to decode obfuscated strings and information	
T1497 - Virtualization/ Sandbox Evasion	Zloader downloader scripts check if it is running in a virtual environment and will not execute properly if it is	
Credential Access	T1056 - Input Capture	Zloader captures keystrokes on browsers
T1539 - Steal Web Session Cookie	Zloader steals cookies from Chrome, Firefox, and Internet Explorer	

Discovery	T1083 - File and Directory Discovery	Zloader steals cookies by discovering files from specific directories like \Mozilla\Firefox\Profiles
T1012 - Query Registry		
Collection	T1185 - Man in the Browser	Zloader has to install its own (fake) certificate, and has to run a local proxy before deploying a Man-In-TheBrowser (MITB) attack
T1179 - Hooking		

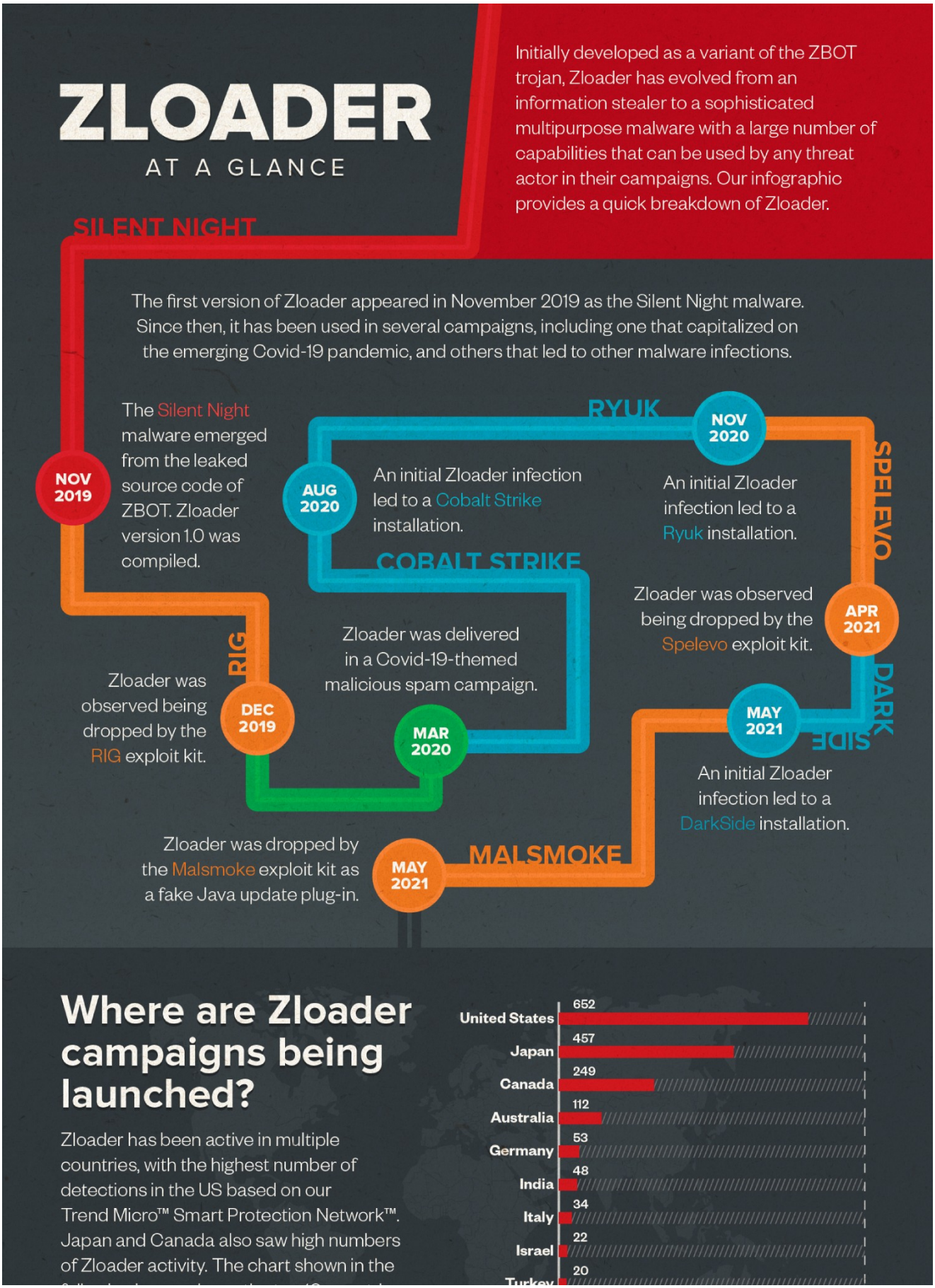
Command & Control	T1001 - Data Obfuscation	C2 is encrypted via RC4 and XORing algorithm where each character of the string is XORed with the preceding character which was already XORed

T1090 - Proxy	Zloader components injected into browsers are responsible for redirecting traffic via proxy	
T1071- Application Layer Protocol	The following commands are accepted: user_execute - download an executable into the %TEMP% folder and run it (optionally with parameters) user_cookies_get - steal cookies from all known browsers user_url_block - block URL access for the current user bot_uninstall - complete removal of the bot from the current user user_password_get – steal passwords from targeted browsers user_files_get – search and upload documents of the victims (.txt, docx,, .xls, .wallet.dat)	
T1219 - Remote Access Software	Zloader downloads and executes VNC tool to control victim machine	
Exfiltration	T1041 - Exfiltration Over C&C Channel	Data collected by Zloader, such as stolen cookies, screenshot, and process list, are exfiltrated to C&C server

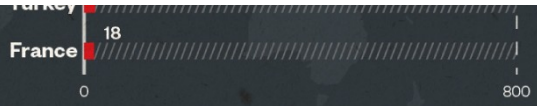
Indicators of Compromise

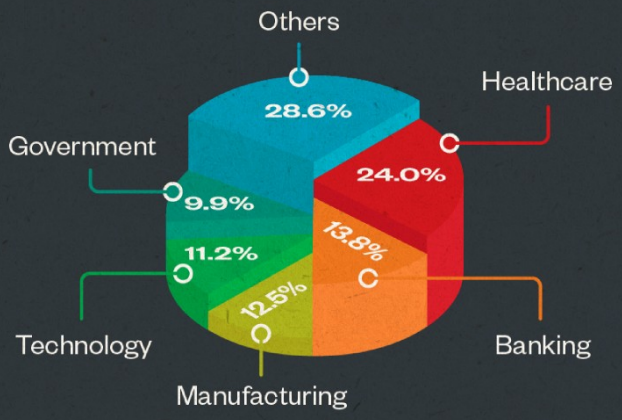
The IOCs for Zloader can be found in this appendix.

HIDE


ZLOADER
AT A GLANCE
Initially developed as a variant of the ZBOT trojan, Zloader has evolved from an information stealer to a sophisticated multipurpose malware with a large number of capabilities that can be used by any threat actor in their campaigns. Our infographic provides a quick breakdown of Zloader.
SILENT NIGHT
The first version of Zloader appeared in November 2019 as the Silent Night malware. Since then, it has been used in several campaigns, including one that capitalized on the emerging Covid-19 pandemic, and others that led to other malware infections.
NOV 2019
The Silent Night malware emerged from the leaked source code of ZBOT. Zloader version 1.0 was compiled.
RIG
DEC 2019
Zloader was observed being dropped by the RIG exploit kit.
COBALT STRIKE
AUG 2020
An initial Zloader infection led to a Cobalt Strike installation.
MAR 2020
Zloader was delivered in a Covid-19-themed malicious spam campaign.
RYUK
NOV 2020
An initial Zloader infection led to a Ryuk installation.
SPELEVO
APR 2021
Zloader was observed being dropped by the Spelevo exploit kit.
DARK SIDE
MAY 2021
An initial Zloader infection led to a DarkSide installation.
MALSMOKE
MAY 2021
Zloader was dropped by the Malsmoke exploit kit as a fake Java update plug-in.
Where are Zloader campaigns being launched?
Zloader has been active in multiple countries, with the highest number of detections in the US based on our Trend Micro™ Smart Protection Network™. Japan and Canada also saw high numbers of Zloader activity. The chart shown in the
United States 652
Japan 457
Canada 249
Australia 112
Germany 53
India 48
Italy 34
Israel 22
Turkey 20

following image shows the top 10 countries with the greatest number of detections from January to August 2021.



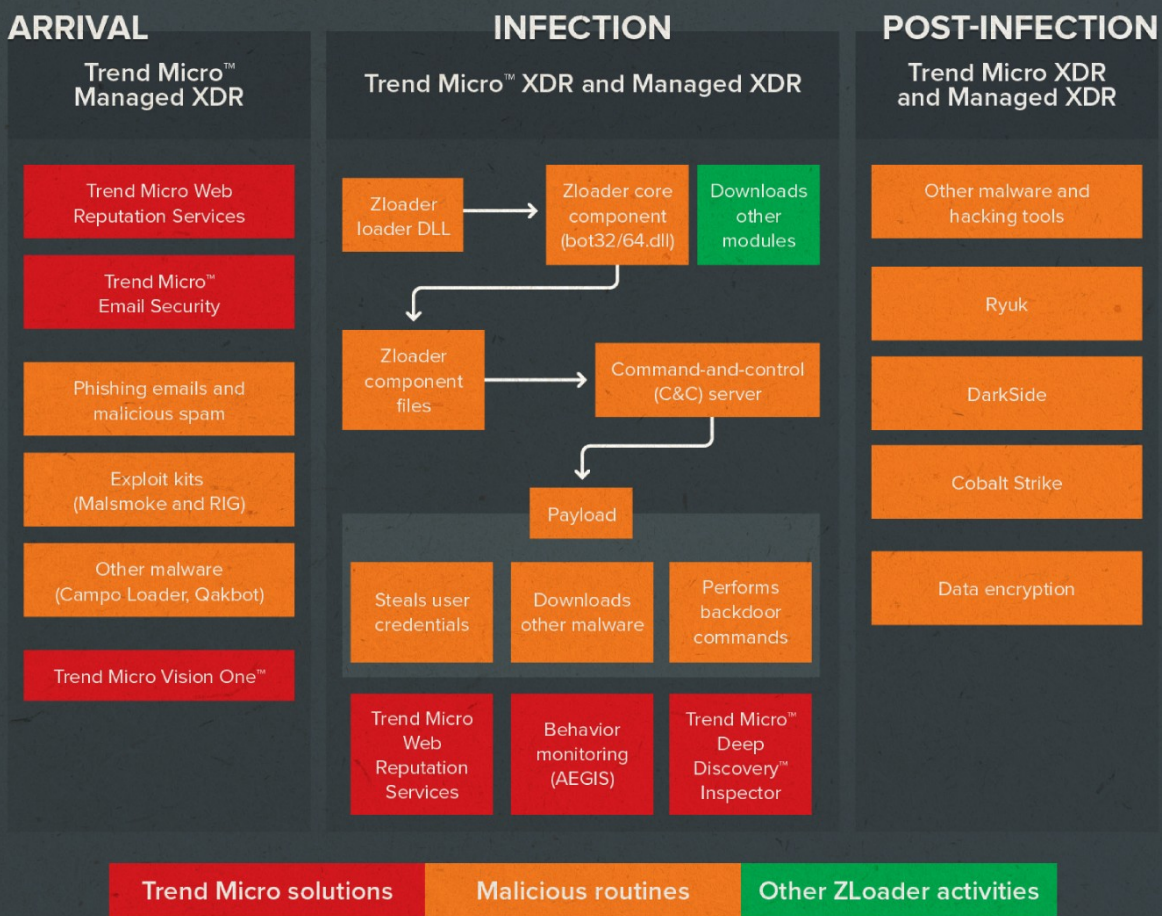


Which industries are being targeted by Zloader campaigns?

Healthcare is the industry with the highest number of Zloader detections, followed by banking, manufacturing, technology, and government. In general, Zloader has been used in campaigns against several major industries.

Infection routine

Zloader arrives via various delivery methods and can result in infected systems having their data stolen or being exposed to new malware infections. Organizations can defend themselves against these attacks by using security solutions powered by AI and machine-learning (ML) technologies, as well as through multilayered security approaches.

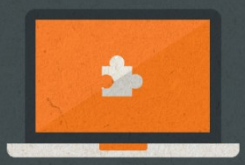


Impact of a Zloader attack

Zloader also has a number of capabilities. In addition to information theft, it can also have the capability to allow ransomware and other malicious tools to enter the systems of its target.

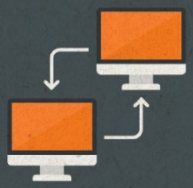
Additional payloads

Enables the entry of other malware and tools like Cobalt Strike and Ryuk



Additional plug-ins

Additional plug-ins can be installed to perform routines such as reading and stealing cookies from browsers.



Remote access

Certain Zloader component files allow the opening of hidden VNC connections to the victim machine.

Browser form data theft

Enables theft of sensitive data from web browsers

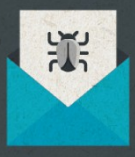
Web injection

Another method of stealing data from web browsers

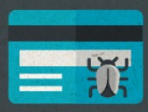
Other malware and tools used in Zloader campaigns

Zloader can be dropped by various hacking tools and can also download other malware or tools such as Ryuk and DarkSide.

DROPS ZLOADER



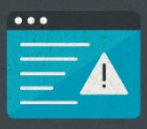
Campo Loader



Qakbot

ZLOADER POST-INFECTION MALWARE

Ryuk



Cobalt Strike

DarkSide

Trend Micro Research is powered by experts who are passionate about discovering and anticipating new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative and thought-provoking research.

TREND MICRO | research

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Infographics, Targeted Attacks