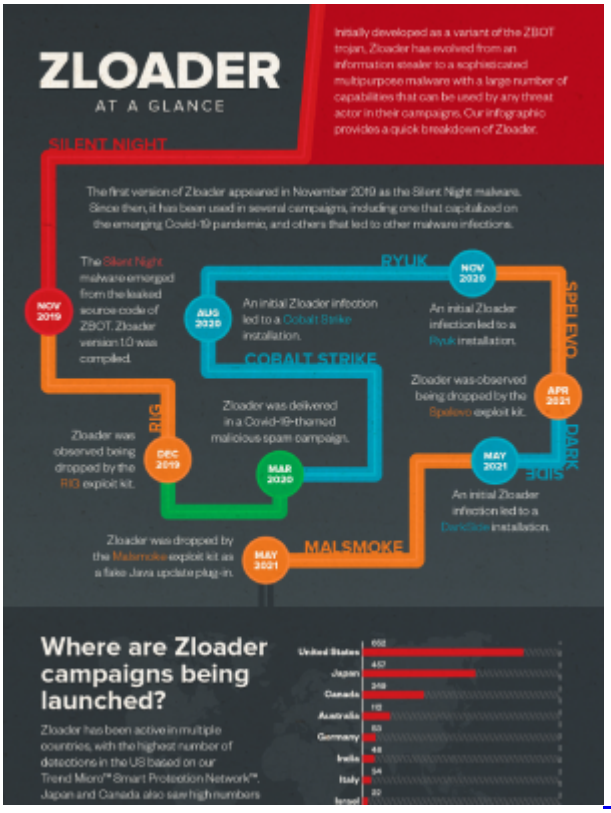
Zloader Campaigns at a Glance

Archived: 2026-04-05 16:59:37 UTC



open on a new tabView 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 2006news- cybercrime-and-digital-threats, 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 Nightopen on a new tab 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™products, 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 XDRservices, 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.

Indicators of Compromise

The IOCs for Zloader can be found in this appendixopen on a new tab.

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

MAR 2020 — Zloader was delivered in a Covid-19-themed malicious spam campaign.

AUG 2020 — An initial Zloader infection led to a Cobalt Strike installation.

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

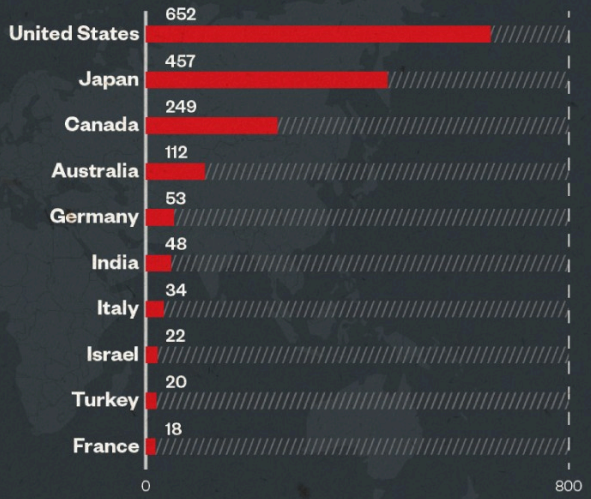
MAY 2021 — An initial Zloader infection led to a DarkSide installation.

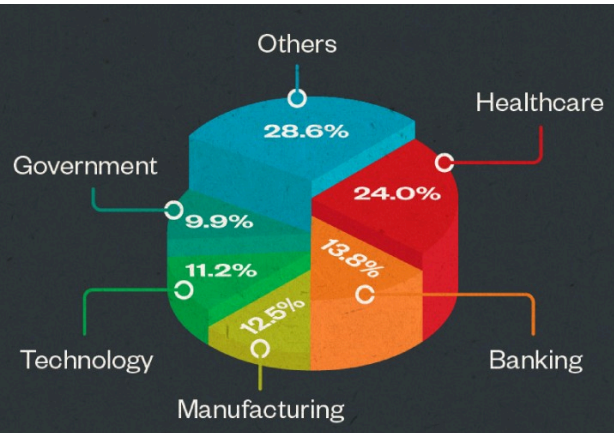
MALSMOKE

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



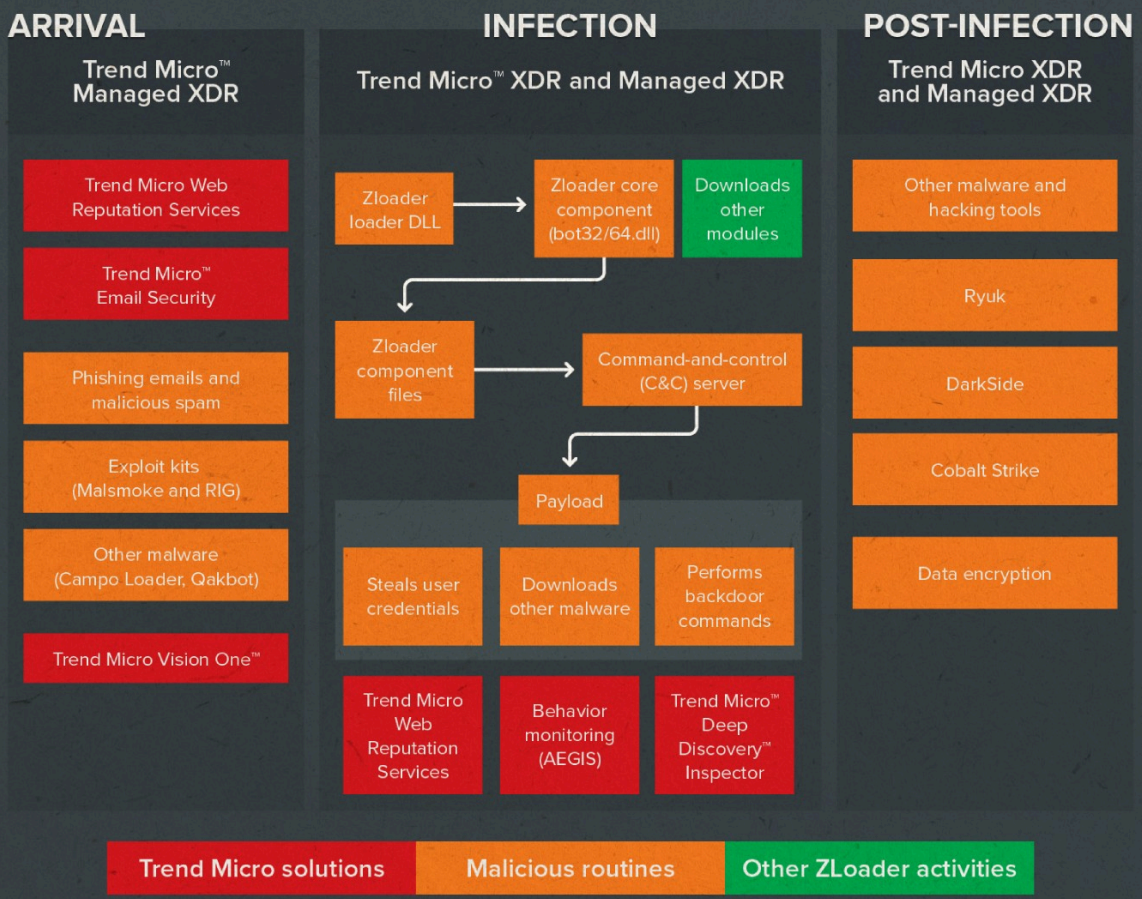


Which industries are being targeted by Zloader campaigns?

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

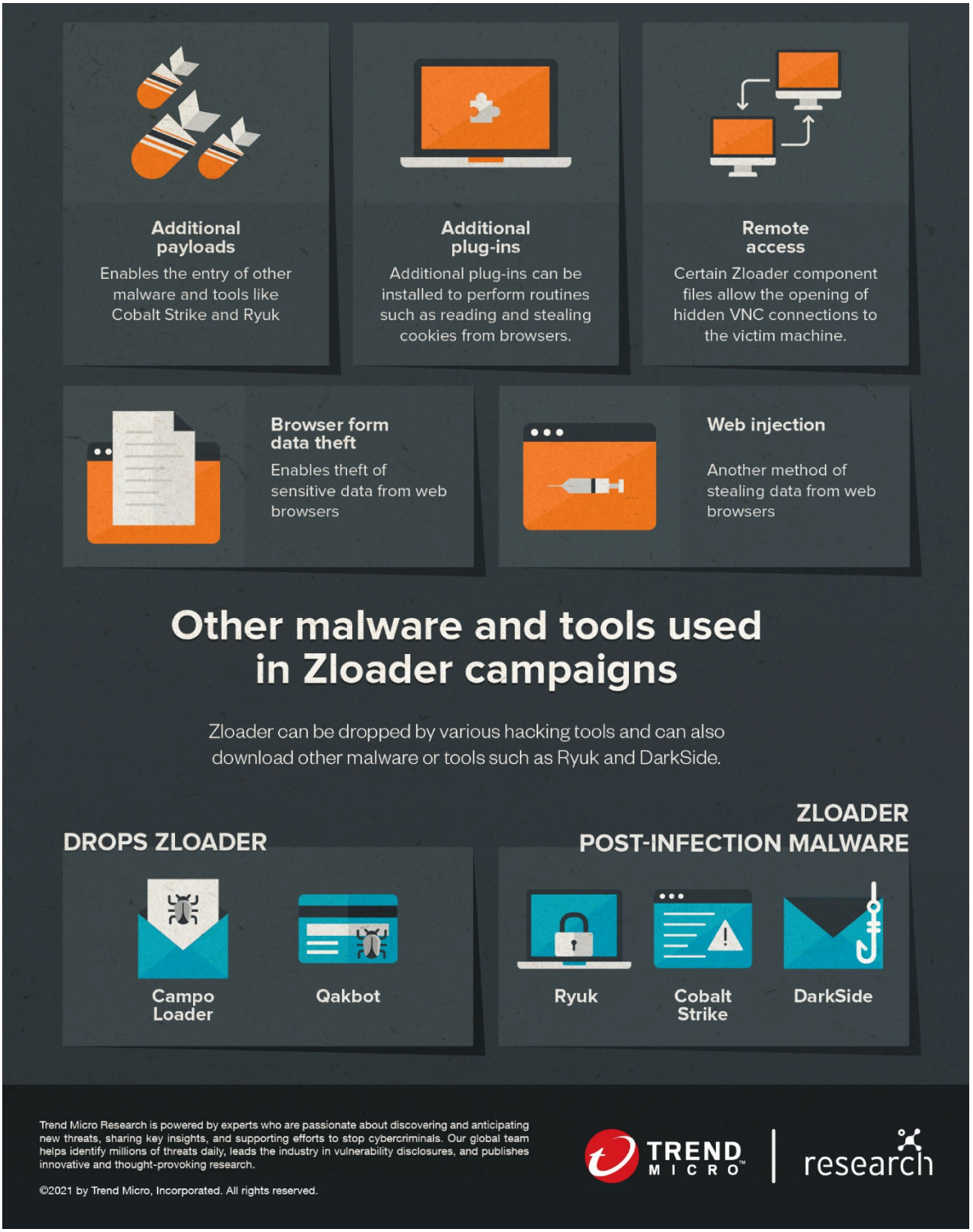
Zloader arrives via various delivery methods and can result in infected systems having their data stolen or being exposed to new malware infections. Organizations can defend themselves against these attacks by using security solutions powered by AI and machine-learning (ML) technologies, as well as through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



Trend Micro solutions | Malicious routines | Other ZLoader activities

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.



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.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---