Share

ESET researchers provided technical analysis, statistical information, and known command and control server domain names and IP addresses

ESET has collaborated with partners Microsoft's Digital Crimes Unit, Lumen's Black Lotus Labs, Palo Alto Networks Unit 42, and others in an attempt to disrupt known Zloader botnets. ESET contributed to the project by providing technical analysis, statistical information, and known command and control server domain names and IP addresses.

Zloader started life as a banking trojan, but lately evolved to become a distributor of several malware families, including various ransomware families.

The coordinated disruption operation targeted three specific botnets, each one using a different version of the Zloader malware. ESET researchers helped with identification of 65 domains that had been used by these botnet operators recently and that had been taken over for this disruption operation to be effective. On top of that, Zloader bots rely on a backup communication channel that automatically generates unique domain names that can be used to receive commands from their botmasters. This technique, known as a domain generation algorithm (DGA), is used to generate 32 different domains per day, per botnet. To make sure that the botnet operators cannot use this side channel to regain control of their botnets, additional 319 already registered domains generated by this algorithm were taken over and the working group is also taking measures to block registration of DGA domains possibly generated in the future. Microsoft's investigation also identified Denis Malikov as a co-author of a malicious component used by the operators of one of the botnets.

Background

Zloader is one of the many banking trojan malware families heavily inspired by the famous Zeus banking trojan, whose source code was leaked in 2011. Many research papers have been published about this malware already, with the latest one from Malwarebytes and HYAS being the most detailed from the technical point of view.

This blogpost won't focus on deep technical aspects of the trojan, but rather will cover the details of its operation and infrastructure.

The first version (1.0.0.0) of Zloader that we were able to find was compiled on November 9th 2019, the same day it was announced and advertised in underground forums under the name "Silent Night". ESET researchers have been closely monitoring its activity and evolution ever since then, giving us great insight into Zloader's mode of operation and its infrastructure.

Throughout Zloader's existence, we have analyzed about 14,000 unique samples via our automatic tracking system, which helped us to discover more than 1,300 unique C&C servers. In March 2020, Zloader implemented a domain generation algorithm (DGA) that allowed us to discover about 300 additional active domains registered by Zloader operators and used as C&C servers.

We have seen a couple of peaks in Zloader's popularity among threat actors, mainly during its first year of existence, but its use began declining during 2021 with only a couple of actors left using it for their malicious intents. This may, however, change in the future as we have already seen version 2.0 samples in the wild (compiled in July 2021). Our findings show that these were just test builds, but we will be closely monitoring this new activity and its evolution. Due to low prevalence and the nature of this new version, all the following information applies to Zloader version 1.x.

As already mentioned, Zloader, similar to other commodity malware, is being advertised and sold on underground forums. When purchased, affiliates are given all they need to set up their own servers with administration panels and to start building their bots. Affiliates are then responsible for bot distribution and maintaining their botnets.

As you can see in Figure 1, we have observed Zloader infestations and campaigns in many countries with North America being the most targeted.

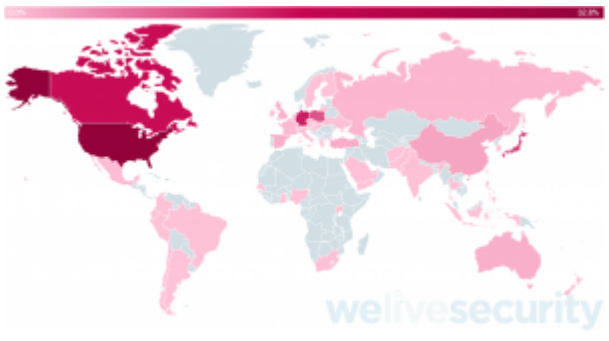

Figure 1. Worldwide Zloader campaign detection rate (based on data since February 2020)

Zloader has been used by various affiliate groups and each of them has used a different approach for the malware's distribution, including:

- RIG exploit kit
- COVID-19-themed spam emails with malicious Microsoft Word documents attached

- Variants of a fake invoice spam emails with malicious XLS macros
- Misuse of Google Ads

The development of the latest distribution methods will be covered in the next sections.

Zloader internals

Zloader has a modular architecture, downloading and utilizing its modules as needed. Supported Zloader modules are displayed in Table 1 and Table 2.

Table 1. Overview of malicious modules used by Zloader

Malicious modules	Functionality
Loader module	Loading the core module
Core module (x86)	Main functionality for x86 processes
Core module (x64)	Main functionality for x64 processes
hvnc32 module	Hidden VNC (x86) for remote PC control
hvnc64 module	Hidden VNC (x64) for remote PC control

Table 2. Legitimate tools abused by Zloader to support its malicious tasks

Helper modules	Functionality
zlib1.dll	Used to support AitB attacks
libssl.dll	Used to support AitB attacks
certutil.exe (+necessary DLL files)	Used to support AitB attacks
sqlite3.dll	Used for processing browser data

Zloader's first component is a loader that is used to download or load (if already downloaded) the core module. This core module is then responsible for downloading and loading additional modules and performing its own malicious tasks.

Zloader's notable features are:

- Ability to steal various data from browsers and Microsoft Outlook, steal cryptocurrency wallets
- Keystroke logging
- HiddenVNC support to allow the operator to remotely control compromised systems
- Support for Zeus-like webinjects, form grabbing and form screenshotting
- Arbitrary command execution (e.g., download and execute other malware)

All communication between bots and their C&C servers is performed over HTTP/HTTPS, and regardless of which is used the data is encrypted using RC4. Some of the data is additionally encrypted using an XOR-based algorithm known as "Visual Encrypt". The RC4 key is unique for each affiliate as described in the next section. Figure 2 shows a bot's static configuration. It contains a list of up to ten hardcoded C&C URLs along with other important data for communication — such as the botnetID to help the operator easily filter data from different campaigns, the signature for communications verification, etc. A bot's C&C list can be easily updated by issuing a command from the operator's administration panel if needed.

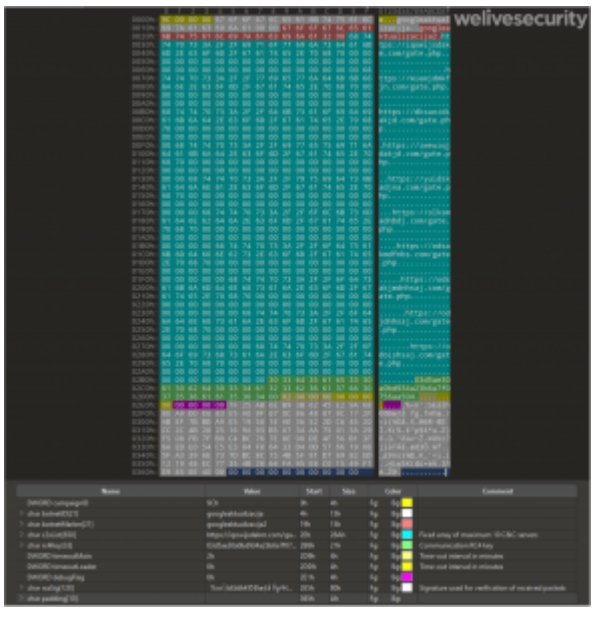

Figure 2. Zloader's static configuration

If none of the hardcoded servers responds, a Zloader bot can use its DGA as a fallback mechanism. Every day, a list of 32 new domains unique for every affiliate is generated based on the current day retrieved by GetLocalTime function. Generated URLs have the format https://<20_random_lowercase_ASCII_letters>.com/post.php

Botnet infrastructure and affiliates

The RC4 encryption key used in botnet communication is unique for every affiliate and tied to the affiliate's administration panel installation. This uniqueness gives us the opportunity to cluster Zloader samples and track affiliates' distribution methods and the evolution of their campaigns.

Since the beginning of our tracking, we have observed more than 25 different RC4 keys. It is worth noting that some of these affiliates were active for a very short period — some of them were probably just testing Zloader's features. It is also possible that some operators just redeployed their administration panel installation at some point and continued their operation with a new RC4 key. A timeline of notable affiliate activity, as well as various Zloader version release dates, can be seen in Figure 3.

Figure 3. Activity of some of the notable affiliates

As can be seen in Figure 5, from October 2020, most Zloader activity was due to only two affiliates. We can distinguish them by their RC4 keys — 03d5ae30a0bd934a23b6a7f0756aa504 and dh8f3@3hdf#hsf23

We cover these two affiliates' activities in the next two sections.

dh8f3@3hdf#hsf23

This affiliate was active under this particular RC4 key starting in June 2020. The first Zloader version it used was 1.3.27.0 and then closely followed the newest version available up until the latest available Zloader version to this date — 1.8.30.0. However, its activity started to decline in the second half of 2021 and we haven't seen any new activity of this botnet since late November 2021.

One of the most interesting activities of this affiliate is that it used Zloader's ability to deploy arbitrary payloads to distribute malicious payloads to its bots. Most notably, it spread various ransomware families such as DarkSide, as highlighted by this research from Guidepoint Security. However, the botmaster did not deploy ransomware to all of their bots; they deployed this type of malware mostly on systems belonging to corporate networks. When installed on a system, Zloader gathers various information about the network its compromised host belongs to. This allows botnet operators to pick specific payloads depending on the victim's network.

This affiliate was spreading their malicious Zloader samples mostly through spam emails with malicious documents attached to them. The Zloader static configuration contains a botnetID, allowing the botmaster to cluster different bots in different sub-botnets. The most prevalent botnetIDs for this affiliate in the last year of its operation were nut and kev.

This operator was also a bit more security aware compared to other Zloader customers and used a tiered architecture for their C&C servers. Typically, a simple proxy script was planted on an often legitimate but compromised website and it was used for tier1 C&C URLs in their bots. This script simply forwards all HTTP/HTTPS traffic from the bot onto the tier2 server, keeping the location of the real administration panel installation secret.

Besides using Zloader as an entry point for ransomware attacks, this affiliate also used Zloader's adversary-in-the-browser (AitB) capabilities to steal victim information and alter the content of various financial institutions and e-commerce websites based in the USA and Canada.

03d5ae30a0bd934a23b6a7f0756aa504

This affiliate has been using Zloader since its early versions and is still active as of today. Despite the latest available version of Zloader being 1.8.30.0, this affiliate has stuck with version 1.6.28.0 since its release in October 2020. We can only speculate as to the reasons behind this. One hypothesis is that this affiliate did not pay to extend their support coverage for Zloader and thus does not have access to later versions.

The operator of this botnet used to depend solely on C&C domains generated by Zloader's DGA and did not update their bots with a new C&C list for more than a year, meaning that all hardcoded C&C servers in their bots were inactive for a long time. This changed in November 2021 when this affiliate updated their bots with a list of new C&C servers and also updated the static configuration of newly distributed binaries to reflect this change.

This effort was probably motivated by the fear of losing access to their botnet should anyone register and sinkhole all future DGA-generated domains for this actor.

Figure 4 shows the administration panel login page which was installed directly on the C&C server hardcoded in the bot's static configuration.

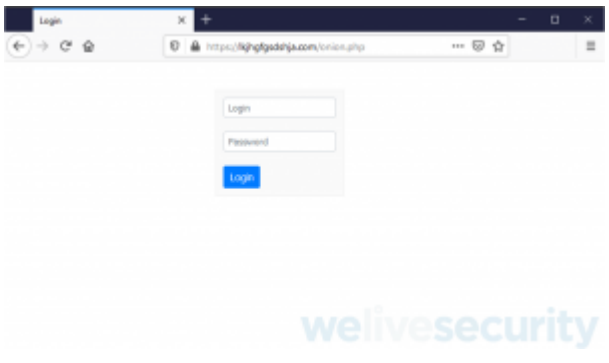

Figure 4. Administration panel login page

Some notable botnetIDs used by this operator were: personal, googleaktualizacija and more recently return, 909222, 9092ti and 9092us.

Through analysis of the webinjects downloaded by the bots in this affiliate botnet, the operator's interests are very broad. They are apparently interested in gathering victim's login credentials and other personal data from various financial institution websites (banks, stock trading platforms, etc.), e-commerce sites (such as Amazon, Best Buy, Walmart), cryptocurrency exchanges and even various online platforms such as Google and Microsoft. Particular focus was put on customers of financial institutions from the USA, Canada, Japan, Australia and Germany.

Additional to the login credential harvesting, this affiliate also used Zloader to distribute various malware families such as the infostealer Raccoon.

Distribution

This threat actor uses various means to spread Zloader with misusing Google Ads and bogus adult sites being their latest distribution methods of choice.

Starting in October 2020, fake adult sites started to push to their visitors malicious payloads posing as a Java update in an MSI package (with filename JavaPlug-in.msi), supposedly required to watch the requested video. This fake Java update package typically contained a downloader that downloaded Zloader itself as the final payload. Since April 2021, this scheme has been enhanced by adding a script to disable Microsoft Defender to further increase the chances of successfully compromising the system.

In June 2021, this affiliate also started to promote packages typically used in corporate environments. When internet users searched for a popular application to download, such as Zoom or TeamViewer, they might have been presented with a fake download site promoted via a Google Ad that tried to trick them into downloading a malicious package posing as the app they were searching for. This distribution method not only installed Zloader but could also install other potentially malicious tools, notably if the compromised system was part of an Active Directory domain. Notorious Cobalt Strike Beacon and Atera Agent were seen to be installed in such cases. These tools could grant the attacker complete control of the compromised system and may result in stealing of sensitive company data, installation of other malware such as ransomware and other malicious activity incurring significant losses for the company.

Figure 5 shows the logic to check if a system belongs to a domain. As seen below, Cobalt Strike Beacon is installed if the list of the system's trusted domains is non-empty.

Figure 5. PowerShell script responsible for Cobalt Strike Beacon installation

The latest iteration of this distribution method relied heavily on the aforementioned Atera Agent, which was usually downloaded from bogus adult sites. An example of what a visitor would see is shown in Figure 6.

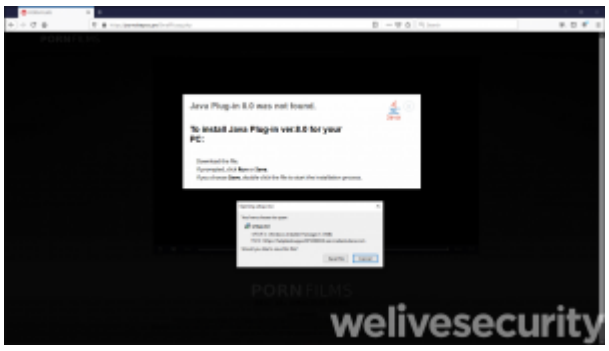

Figure 6. Fake adult site luring users into downloading Atera remote management tool

Atera Agent is a legitimate “remote monitoring and management” solution used by IT companies to administer their customers’ systems. One of its features — remote script execution — was used in this campaign to deliver Zloader payloads and other malicious helper files. The purpose of these helper files was to support the installation process by executing specific tasks such as privilege escalation, execution of further sample, disabling of Windows Defender, etc.

These tasks were usually achieved via simple BAT files, but it is worth mentioning that attackers also exploited a known digital signature verification vulnerability to use legitimate, signed Windows executable files with malicious VBScripts appended to the end of the file, where the signature section is located (see Figure 7). For the PE file to remain valid, attackers also need to alter the PE header to alter the signature section length and checksum. This alteration of the file’s content does not revoke the validity of its digital signature during the verification process because the modified content is exempted from the verification process. Thus, the file’s new malicious content may therefore stay off the radar. This vulnerability is described, for example, in CVE-2012-0151 or CVE-2013-3900, and also in this blogpost by Check Point Research. Its fix is unfortunately disabled by default in Windows, and therefore, it still can be misused by attackers in a large number of systems.

Figure 7. Example of a script appended to the PE file signature section

In the recent campaign, a Ursnif trojan was sometimes installed instead of Zloader, showing that this affiliate group does not rely on a single malware family but has more tricks up its sleeve. A typical scenario of this distribution method is displayed in Figure 8.

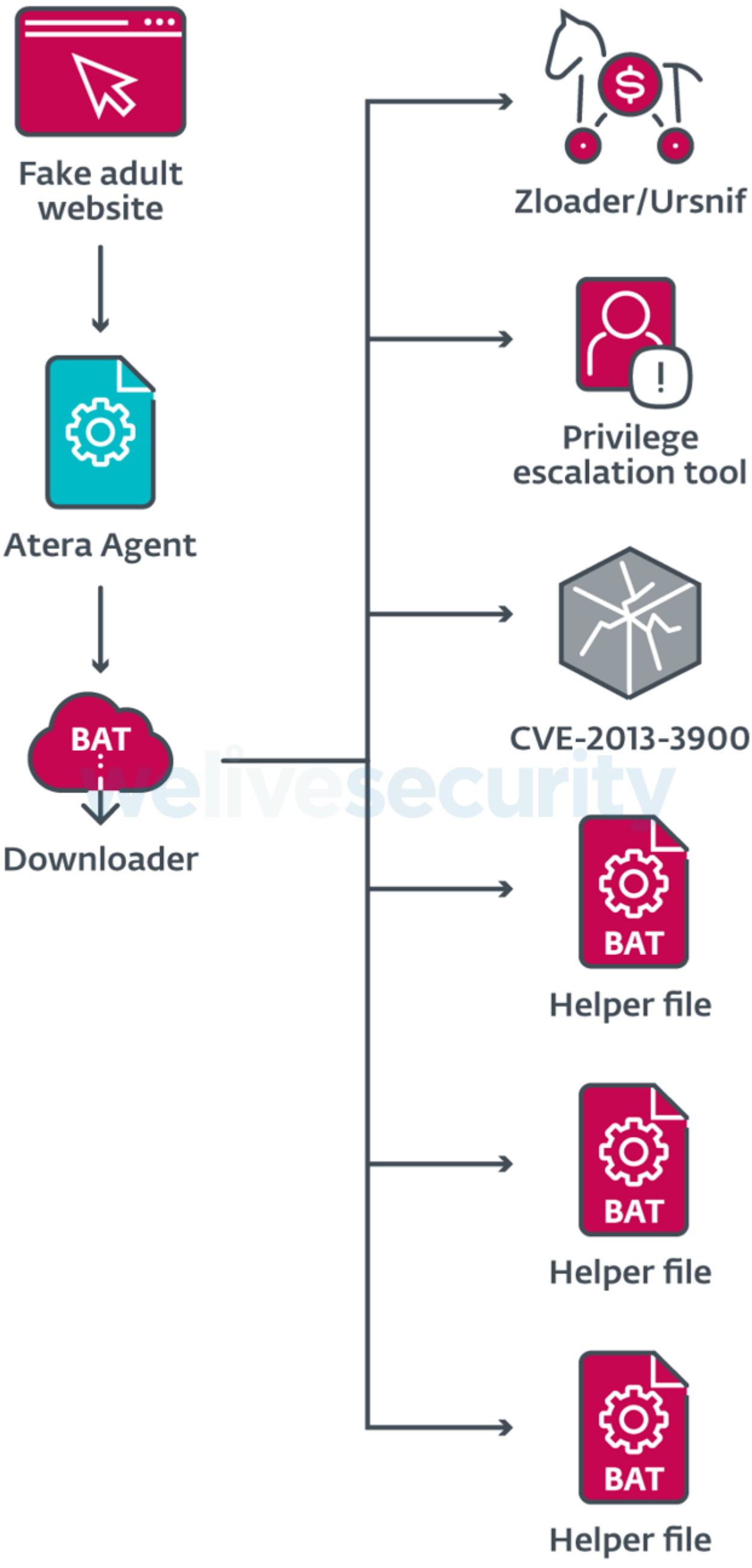

Figure 8. Typical distribution method using Atera Agent

Closing remarks

We relentlessly continue to track threats that are used to spread ransomware, which is an ongoing threat to internet security. As Zloader is available in underground forums, ESET Researchers will monitor any new activity tied to this malware family, following this disruption operation against its existing botnets.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.

ESET Research now also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

Samples

SHA-1	Filename	ESET detection name	Description
4858BC02452A266EA3E1A0DD84A31FA050134FB8	9092.dll	Win32/Kryptik.HNLQ trojan	Zloader return botnet as downloaded from https://teamworks455[.]com/_country/check.php
BEAB91A74563DF8049A894D5A2542DD8843553C2	9092.dll us.dll	Win32/Kryptik.HODI trojan	Zloader 9092us botnet as downloaded from https://endoftheendi[.]com/us.dll
462E242EF2E6BAD389DAB845C68DD41493F91C89	N/A	Win32/Spy.Zbot.ADI trojan	Unpacked initial loader component of 9092us botnet.
30D8BA32DAF9E18E9E3CE564FC117A2FAF738405	N/A	Win32/Spy.Zbot.ADI trojan	Downloaded Zloader main core component (x86).
BD989516F902C0B4AFF7BCF32DB511452355D7C5	N/A	Win64/Spy.Zbot.Q trojan	Downloaded Zloader main core component (x64).
E7D7BE1F1FE04F6708EFB8F0F258471D856F8F8F	N/A	Win32/Hvnc.AO trojan	Downloaded Zloader HVNC component (x86).
5AA2F377C73A0E73E7E81A606CA35BC07331EF51	N/A	Win64/Hvnc.AK trojan	Downloaded Zloader HVNC component (x64).
23D38E876772A4E28F1B8B6AAF03E18C7CFE5757	auto.bat	BAT/Agent.PHM trojan	Script used by Atera Agent distribution method.
9D3E6B2F91547D891F0716004358A8952479C14D	new.bat	BAT/Agent.PHL trojan	Script used by Atera Agent distribution method.
33FD41E6FD2CCF3DFB0FCB90EB7F27E5EAB2A0B3	new1.bat	BAT/Shutdown.NKA trojan	Script used by Atera Agent distribution method.
5A4E5EE60CB674B2BFCD583EE3641D7825D78221	new2.bat	BAT/Shutdown.NKA trojan	Script used by Atera Agent distribution method.
3A80A49EFAAC5D839400E4FB8F803243FB39A513	adminpriv.exe	Win64/NSudo.A potentially unsafe application	NSudo tool used for privilege escalation by distribution scripts.
F3B3CF03801527C24F9059F475A9D87E5392DAE9	reboot.dll	Win32/Agent.ADUM trojan	Signed file exploiting CVE-2013-3900 to hide malicious script commands.
A187D9C0B4BDB4D0B5C1D2BDBCB65090DCEE5D8C	TeamViewer.msi	Win64/TrojanDownloader.Agent.KY trojan	Malicious MSI installer containing downloader used to deliver Zloader.
F4879EB2C159C4E73139D1AC5D5C8862AF8F1719	tvlauncher.exe	Win64/TrojanDownloader.Agent.KY trojan	Downloader used to deliver Zloader.
E4274681989347FABB22050A5AD14FE66FFDC000	12.exe	Win32/Kryptik.HOGN trojan	Raccoon infostealer downloaded by Zloader.

SHA-1	Filename	ESET detection name	Description
FA1DB6808D4B4D58DE6F7798A807DD4BEA5B9BF7	racoon.exe	Win32/Kryptik.HODI trojan	Raccoon infostealer downloaded by Zloader.

Network

Domains and URLs used in distribution

- https://endoftheendi[.]com
- https://sofftsportal[.]su
- https://pornokeyxxx[.]pw
- https://porno3xgirls[.]website
- https://porno3xgirls[.]space
- https://porno3xgirls[.]fun
- https://porxnoxxx[.]site
- https://porxnoxxx[.]pw
- https://pornoxxxguru[.]space
- https://helpdesksupport072089339.servicedesk.atera[.]com/GetAgent/Msi/?customerId=1&integratorLogin=izunogg1017@gmail.com
- https://helpdesksupport350061558.servicedesk.atera[.]com/GetAgent/Msi/?customerId=1&integratorLogin=Ario.hi@rover.info
- https://clouds222[.]com
- https://teamworks455[.]com
- https://commandaadmin[.]com
- https://cmdadminu[.]com
- https://checksoftupdate[.]com
- https://datalystoy[.]com
- https://updatemsicheck[.]com

Latest Zloader C&C servers

- https://asdfghdsajkl[.]com/gate.php
- https://lkjhgfgsdshja[.]com/gate.php
- https://kjdhsasghjds[.]com/gate.php
- https://kdjwhqejqwij[.]com/gate.php
- https://iasudjghnasd[.]com/gate.php
- https://daksjuggdhwa[.]com/gate.php
- https://dkisuaggdjhna[.]com/gate.php
- https://eiqwuggejqw[.]com/gate.php
- https://dquggwjhdmq[.]com/gate.php
- https://djshggadasj[.]com/gate.php

URLs used to download arbitrary malware

- https://braves[.]fun/racoon.exe
- https://endoftheendi[.]com/12.exe

Domains used in recent Zloader's Webinjects attacks

- https://dotxvcnjlvdajkwerwoh[.]com
- https://aerulonoured[.]su
- https://rec.kindplanet[.]us

MITRE ATT&CK techniques

This table was built using version 10 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	Several domains were acquired to support C&C.
	T1583.004	Acquire Infrastructure: Server	Several servers were used to host Zloader infrastructure.
	T1584.004	Compromise Infrastructure: Server	Some legitimate websites were compromised to host parts of Zloader infrastructure.
	T1587.001	Develop Capabilities: Malware	Zloader is malware targeting users of the Windows operating system.
	T1587.002	Develop Capabilities: Code Signing Certificates	Some of the distribution methods use signed malicious binaries.
	T1587.003	Develop Capabilities: Digital Certificates	Digital certificates are used in HTTPS traffic.
	T1588.001	Obtain Capabilities: Malware	Various malware samples are used to distribute Zloader or are distributed by Zloader itself.
	T1588.002	Obtain Capabilities: Tool	Various legitimate tools and libraries are used to support Zloader tasks.
	T1588.006	Obtain Capabilities: Vulnerabilities	CVE-2013-3900 is exploited in one of the distribution methods.
Initial Access	T1189	Drive-by Compromise	Google Ads and fake websites are used to lure victims into downloading malicious installers.
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	PowerShell commands are used to support some distribution methods.
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Batch files are used to support some distribution methods.
	T1059.005	Command and Scripting Interpreter: Visual Basic	VBScript is used to launch main Zloader payload.
	T1106	Native API	Zloader makes heavy use of dynamic Windows API resolution.
	T1204.001	User Execution: Malicious Link	Zloader is commonly distributed through malicious links.
	T1204.002	User Execution: Malicious File	Zloader is commonly distributed via malicious MSI installers.
	T1047	Windows Management Instrumentation	Zloader uses WMI to gather various system information.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Zloader uses registry run key to establish persistence.
Privilege Escalation	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Several methods are used to bypass UAC mechanisms.
	T1055.001	Process Injection: Dynamic-link Library Injection	Zloader injects its modules into several processes.
	T1140	Deobfuscate/Decode Files or Information	Zloader stores its modules in an encrypted form to hide their presence.
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools	Some distribution methods disable Windows Defender prior to the installation of Zloader.
	T1070.004	Indicator Removal on Host: File Deletion	Some components of Zloader or its distribution method are removed after successful installation.
	T1036.001	Masquerading: Invalid Code Signature	Some installers have been signed using invalid certificates to make them seem more legitimate.
	T1036.005	Masquerading: Match Legitimate Name or Location	Some installers mimic names of legitimate applications.
	T1027.002	Obfuscated Files or Information: Software Packing	Zloader's code is obfuscated and its payload is usually packed.
	T1553.004	Subvert Trust Controls: Install Root Certificate	Browser certificates are installed to support AitB attack.
Credential Access	T1557	Adversary-in-the-Middle	Zloader leverages AitB techniques to intercept selected HTTP/HTTPS traffic.
	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Zloader can gather saved credentials from browsers.

Tactic	ID	Name	Description
	T1056.001	Input Capture: Keylogging	Zloader can capture keystrokes and send them to its C&C server.
	T1539	Steal Web Session Cookie	Zloader can gather cookies saved by browsers.
	T1482	Domain Trust Discovery	Zloader gathers information about domain trust relationships.
	T1083	File and Directory Discovery	Zloader can search for various documents and cryptocurrency wallets.
	T1057	Process Discovery	Zloader enumerates running processes.
	T1012	Query Registry	Zloader queries registry keys to gather various system information.
Discovery	T1518.001	Software Discovery: Security Software Discovery	A WMI command is used to discover installed security software.
	T1082	System Information Discovery	Zloader gathers various system information and sends it to its C&C.
	T1016	System Network Configuration Discovery	Network interface information is gathered and sent to the C&C.
	T1033	System Owner/User Discovery	Username is used to generate a botID to identify a system in a botnet.
	T1124	System Time Discovery	Information about the system's time zone is sent to the C&C.
	T1560.003	Archive Collected Data: Archive via Custom Method	Zloader uses RC4 and XOR to encrypt data before sending them to the C&C.
Collection	T1005	Data from Local System	Zloader can collect documents and cryptocurrency wallets.
	T1074.001	Data Staged: Local Data Staging	Zloader saves its collected data to file prior to exfiltration.
	T1113	Screen Capture	Zloader has the ability to create screenshots of windows of interest.
	T1071.001	Application Layer Protocol: Web Protocols	Zloader uses HTTP/HTTPS for C&C communication.
	T1568.002	Dynamic Resolution: Domain Generation Algorithms	A DGA is used as a fallback in samples since 2020-03.
Command and Control	T1573.001	Encrypted Channel: Symmetric Cryptography	RC4 is used for C&C traffic encryption. Some of the data is additionally XOR encrypted.
	T1008	Fallback Channels	Multiple C&C servers are usually present in Zloader configurations to avoid relying on just one. A DGA is also implemented.
	T1219	Remote Access Software	HiddenVNC module is used to support remote access.
Exfiltration	T1041	Exfiltration Over C2 Channel	Zloader exfiltrates gathered data over its C&C communication.
	T1490	Inhibit System Recovery	Some of the distribution methods disable Windows recovery function through bcdedit.exe.
Impact	T1489	Service Stop	Some of the distribution methods disable the Windows Defender service.
	T1529	System Shutdown/Reboot	Some of the distribution methods shut down the system after the initial compromise.

Jean-Ian Boutin Tomáš Procházka 13 Apr 2022 - 06:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis — Digital Security Resource Center

Newsletter

Discussion