By Antonio Pirozzi and Antonio Cocomazzi

Executive Summary

- New ZLoader campaign has a stealthier distribution mechanism which deploys a signed dropper with lower rates of detection.
- The campaign primarily targets users of Australian and German banking institutions.
- The new infection chain implements a stager which disables all Windows Defender modules.
- The threat actor uses a backdoored version of the Windows utility `wextract.exe` to embed the ZLoader payload and lower the chance of detection.
- SentinelLabs identified the entire infrastructure of the 'Tim' botnet, composed of more than 350 recently-registered C2 domains.

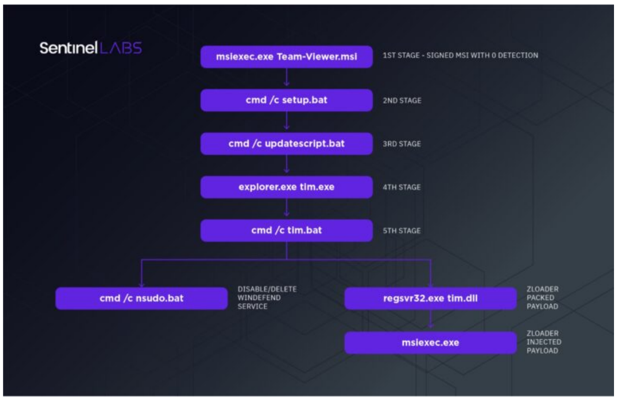
Read the Full Report

Introduction

ZLoader (https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader) (also known as Terdot) was first discovered in 2016 (https://www.fortinet.com/blog/threat-research/the-curious-case-of-an-unknown-trojan-targeting-german-speaking-users) and is a fork of the infamous Zeus banking trojan. It is still under active development. A multitude of different versions have appeared (https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns) since December 2019, with an average frequency of 1-2 new versions released each week.

ZLoader is a typical banking trojan which implements web injection to steal cookies, passwords and any sensitive information. It attacks users of financial institutions all over the world and has also been used to deliver ransomware families like Egregor (https://www.sentinelone.com/labs/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/) and Ryuk (https://www.sentinelone.com/labs/an-inside-look-at-how-ryuk-evolved-its-encryption-and-evasion-techniques/). It also provides backdoor capabilities and acts as a generic loader to deliver other forms of malware. Newer versions (https://www.malwarebytes.com/resources/files/2020/06/the-silent-night-zloader-zbot_final.pdf) implement a VNC module which permits users to open a hidden channel that gives the operators remote access to victim systems. ZLoader relies primarily on dynamic data exchange (DDE) and macro obfuscation to deliver the final payload through crafted documents.

A recent (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/) evolution of the infection chain included the dynamic creation of agents, which download the payload from a remote server. The new infection chain observed by SentinelLabs demonstrates a higher level of stealth by disabling Windows Defender and relying on living-off-the-land (https://www.sentinelone.com/labs/living-off-windows-land-a-new-native-file-downldr/) binaries and scripts (LOLBAS) in order to evade detection. During our investigation, we were also able to map all the new ZLoader C2 infrastructure related to the 'Tim' botnet and identify the scope of the campaign and its objectives, which primarily involved stealing bank credentials from customers of European banks.



Overview of the ZLoader infection chain

Technical Analysis

The malware is downloaded from a Google advertisement published through Google Adwords. In this campaign, the attackers use an indirect way to compromise victims instead of using the classic approach of compromising the victims directly, such as by phishing.

We observed the following pattern of activity that leads to infection:

- The user performs a search on www.google.com to find a website to download the required software from; in our case, we observed a search for "team viewer download".
- The user clicks on an advertisement shown by Google and is redirected to the fake TeamViewer site under the attacker's control.
- The user is tricked into downloading the fake software in a signed MSI format.

Once the user clicks on the advertisement, it will redirect through the aclk (https://www.warriorforum.com/blogs/clint-butler/15012-google-ad-services-pagead-aclk-what-heck.html) page. This redirect demonstrates the attackers usage of Google Adwords to gain traffic:

```
hxxps://www.google.com/aclk?sa=L&ai=DChcSEwiMusngi8_yAhVbbm8EHYpXDh0YABABGg
```

After further navigation (and redirects), the malicious `Team-Viewer.msi` is downloaded from the final URL `hxxps://team-viewer.site/download/Team-Viewer.msi`.

The downloaded file is a fake TeamViewer installer signed on 2021-08-23 10:07:00. It appears that the cybercriminals managed to obtain a valid certificate issued by Flyintellect Inc (https://opengovca.com/corporation/13146341), a Software company in Brampton, Canada. The company was registered on 29th June 2021, suggesting that the threat actor possibly registered the company for the purpose of obtaining those certificates.

Pivoting from this certificate, we were able to spot other samples signed with the same certificate. These other samples suggest that the attackers had multiple campaigns ongoing beyond TeamViewer and which included fakes such as `JavaPlug-in.mis`, `Zoom.mis`, and `discord.msi`.

At the time of writing, these four samples have no detections on VirusTotal (a complete list of IoCs can be found in the full report).

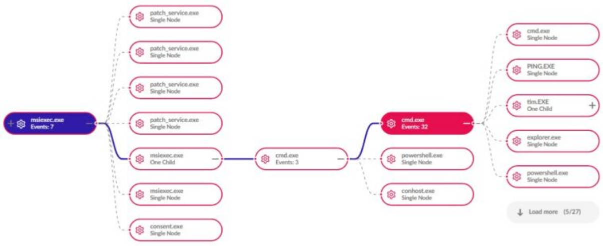
New Zloader Infection Chain Bypass Defences

The `.msi` file is the first stage dropper which runs an installation wizard. It creates random legitimate files in the directory `C:\Program Files (x86)\Sun Technology Network\Oracle Java SE`. Once the folder has been created, it will drop the `setup.bat` file, triggering the initial infection chain by executing `cmd.exe /c setup.bat`.

This initiates the second stage of the infection chain, downloading the dropper `updatescript.bat` through the PowerShell cmdlet `Invoke-WebRequest`, from `hxxps://websekir.com/g00glbat/index/processingSetRequestBat/?servername=msi`. The dropper then executes the third stage with the command `cmd /c updatescript.bat`.

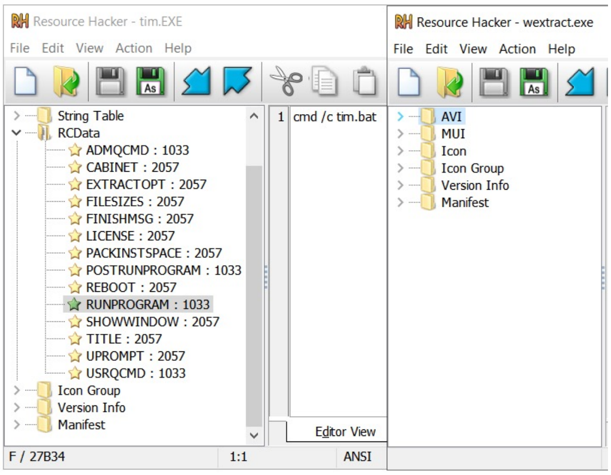
The third stage dropper contains most of the logic to impair the defenses of the machine. It also drops the fourth stage using a stealthy execution technique. At first, it disables all the Windows Defender modules through the PowerShell cmdlet `Set-MpPreference`. It then adds exclusions, such as `regsvr32`, `*.exe`, `*.dll`, with the cmdlet `Add-MpPreference` to hide all the components of the malware from Windows Defender.

At this point the fourth stage dropper is downloaded from the URL `hxxps://pornofilmspremium.com/tim.EXE` and saved as `tim.exe`. The execution of `tim.exe` is done through the LOLBAS (https://lolbas-project.github.io/lolbas/Binaries/Explorer/) command `explorer.exe tim.exe`. This allows the attacker to break the parent/child correlation often used by EDRs for detection.



The first part of the attack chain

The `tim.exe` binary is a backdoored version of the Windows utility `wextract.exe`. This backdoored version contains extra embedded resources with names like "RUNPROGRAM", "REBOOT", and "POSTRUNPROGRAM", among others.



```
cmd /c tim.bat
```

Resources embedded in the `tim.exe` binary (left) and legit `wextract.exe` (right)

This backdoored version contains additional code for creating a new malicious batch file with the name `tim.bat`. It is placed in a temporary directory retrieved with the Win32 function `GetTempPath()`. It retrieves the content of the resource "RUNPROGRAM" (containing the string value `cmd /c tim.bat`) and uses it as the command line parameter for the `CreateProcess()` Win32 function.

The `tim.bat` file is a very short script that downloads the final ZLoader DLL payload with the name `tim.dll` from the URL `hxxps://pornofilmspremium.com/tim.dll` and executes it through the LOLBAS (https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/) command `regsvr32 tim.dll` . This allows the attackers to proxy the execution of the DLL through a signed binary by Microsoft.

This dropper downloads the script `nsudo.bat` from `hxxps://pornofilmspremium.com/nsudo.bat` and runs asynchronously in parallel with the execution of `tim.dll` . The script aims to further impair defenses of the machine.

Privilege Escalation and Defense Evasion

The `nsudo.bat` script performs multiple operations with the goal of elevating privileges on the system and impairing defenses.

At first, it checks if the current context of execution is privileged by verifying the access to the SYSTEM hive. This is done through `%SYSTEMROOT%\system32\cacls.exe %SYSTEMROOT%\system32\config\system` . If the process in which it runs has no access on that hive it will jump to the label `:UACPrompt` .

This part of the script implements an auto elevation VBScript that aims to run an elevated process in order to make system changes. The snippet of the script in charge of the UACPrompt feature is as follows:

```
:UACPrompt
      echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin
      set params = %*:"="
      echo UAC.ShellExecute "cmd.exe", "/c %~s0 %params%", "", "runas", 1 >
        "%temp%\getadmin.vbs"
      del "%temp%\getadmin.vbs"
      exit /B
```

This snippet creates the VBScript `getadmin.vbs` , runs it and deletes it. Using a VBScript eases the interaction with COM objects. In this case, it instantiates a `Shell.Application` object and calls the function `ShellExecute()` to trigger the UAC elevation and the interaction with the AppInfo service.

Once the elevation occurs the script is run with elevated privileges. At this point, the script performs the steps to disable Windows Defender. It does this through a software utility called NSudo (https://nsudo.m2team.org/en-us/) renamed as `javase.exe` , which is downloaded from the URL `hxxps://pornofilmspremium.com/javase.exe` . The attacker leverages this utility in order to spawn a process with “TrustedInstaller” privileges. This can be abused (https://bugs.chromium.org/p/project-zero/issues/detail?id=997) by the attacker to disable the Windows Defender service even if it runs as a Protected Process Light.

The script downloads the file `autorun100.bat` from and places it in the startup folder `%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup` . This script ensures that the WinDefend service is deleted at the next boot through the utility `NSudo` .

The `nsudo.bat` script also completely disables UAC by setting the following registry key to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Syste
```

In order to have these changes take effect, the computer is forced to restart. The `nsudo.bat` script does this with `shutdown.exe /r /f /t 00` . At this point, the attack chain of the script `nsudo.bat` is complete.

ZLoader Payload Execution Chain

The `tim.dll` is the main ZLoader payload that encapsulates the unpacking logic and adds persistence. It is executed through the system signed binary `regsvr32.exe` .

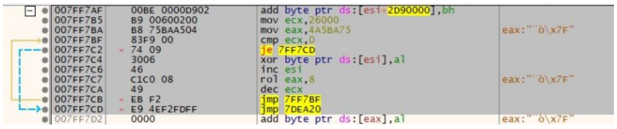
It first creates a directory with a random name inside `%APPDATA%` and then creates a copy of itself in the newly created directory. It then adds a new registry key in `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` . The registry key value contains the command line of the malicious process to spawn on user logon. This ensures that the attacker’s implant survives machine reboots. The DLL execution also relies on the `regsvr32` binary. This is an example of the registry key created on a single run of the sample:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Iwalcacvalu
```

Then it starts the unpacking by leveraging a process injection technique known as Thread Hijacking. It contains a small variation but essentially uses the same pattern of Win32 API calls used for Thread Hijacking:

```
VirtualAllocEx() -> WriteProcessMemory() -> GetThreadContext() -> SetThread
```

It first creates a new process as a host for the unpacked DLL, and for this sample it uses a new instance of `msiexec.exe` . Then it allocates and writes 2 RWX memory regions inside the target process. One contains the unpacked version of the DLL XOR'ed with a key; the second, contains some shellcode to decrypt the DLL and jump to the entry point.

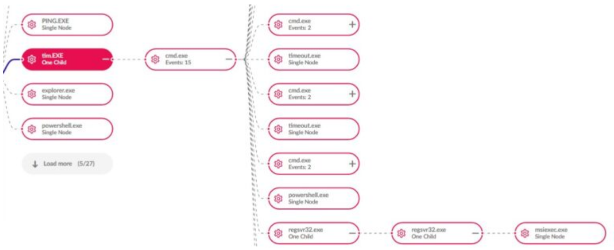


```
007FF7AF     00BE 0000D902     add byte ptr ds:[esi+2D90000],bh
007FF7B5     B9 00600200       mov ecx,26000
007FF7BA     B8 75BAA504       mov eax,4A5BA75              eax:""ò\x7F"
007FF7BF     83F9 00           cmp ecx,0
007FF7C2   ˅ 74 09             je 7FF7CD
007FF7C4     3006              xor byte ptr ds:[esi],al
007FF7C6     46                inc esi
007FF7C7     C1C0 08           rol eax,8                    eax:""ò\x7F"
007FF7CA     49                dec ecx
007FF7CB   ˄ EB F2             jmp 7FF7BF
007FF7CD   ˄ E9 4EF2FDFF       jmp 7DEA20
007FF7D2     0000              add byte ptr ds:[eax],al     eax:""ò\x7F"
```

The unpacking routine

Once the memory is written in the remote process it sets the new thread context EIP to point to the unpacking routine shellcode and resumes the main thread of `msiexec` . This is how the hijacking of the main thread occurs. The unpacked DLL is extracted from the memory of `msiexec.exe` process by dumping the memory address used in the first `WriteProcessMemory()` call.

We have compared the unpacked DLL with the recent ZLoader payloads and found a similarity score of 92.62%.



Final part of the attack chain

Analyzing The New Zloader C2 Infrastructure

The analyzed sample belongs to the 'Tim' Botnet as defined in the malware configuration. Some of the embedded C2s (the full list can be found in the IoC section of the full report) are also shared by the googleaktualizacija (https://tria.ge/210316-7wv57c1c4n) ZLoader botnet.

One of the C2s dumped from the infected machine, `mjwougyhwlgewbajxbnn[.]com` , used to resolve to `194.58.108[.]89` until the 25th of August 2021. As of the 26th of August, however, it points to `195.24.66[.]70` .

The IP `194.58.108[.]89` belongs to ASN 48287 – RU-CENTER and seems to deploy many different domains – 350 at the time of writing – forming the new ZLoader infrastructure. Some domains implement the `gate.php` component, which is a fingerprint of the ZLoader botnet. We noticed during our investigation that all the domains were registered from April to Aug 2021, and they switched to the new IP (`195.24.66[.]70`) on the 26th of August.

A Targeted Campaign: AU And DE Financial Institutions

The new ZLoader campaign is targeted. The final payload has a list of embedded AU and DE domains, and contains some strings with wildcards used by the malware to intercept specific users' web requests to bank portals.

```
@https://*commerzbank.de*
@https://*.de/*/entry*
@https://*.de/banking-*/portal?*
@https://*.de/banking-*/portal;*
@https://*.de/portal/portal*
@https://*.de/privatkunden/*
@https://*.de*abmelden*
@https://*.de/de/home*
@https://*.de/en/home*
@https://*.de/fi/home*
@https://*banking.sparda.de*
@https://*banking.sparda-*
@https://*banking.sparda.de/wps/loggedout.jsp
@https://*meine.deutsche-bank.de/trxm/db*
@https://*banking.berliner-bank.de/trxm*
@https://*meine.norisbank.de/trxm/noris*
@https://*targobank.de*
@https://banking4.anz.com/IBAU/BANKAWAY*
@https://banking.westpac.com.au/*
@https://www1.my.commbank.com.au/netbank/Portfolio/Home/*
@https://ibanking.stgeorge.com.au/ibank/*
@https://ibanking.banksa.com.au/ibank/*
@https://ibanking.bankofmelbourne.com.au/ibank/*
@https://online.macquarie.com.au/*
@https://ob.cua.com.au/ib/*
@https://banking.bendigobank.com.au/banking*
@https://internetbanking.suncorpbank.com.au/*
@https://www.ing.com.au/securebanking/*
@https://ib.nab.com.au/*
@https://online.beyondbank.com.au/*
@https://ib.greater.com.au*
@www.independentreserve.com*
@www.coinspot.com.au*
@https://auth.btcmarkets.net/*
```

From our analysis of the communication patterns related to `mjwougyhwlgewbajxbn[.]com`, we were able to map most of the source traffic used by the operators of the botnet.

The `pornofilmspremium[.]com` domain delivers the `tim.exe` component. The domain was registered on 2021-07-19 (Location RU, ASN: REG RU 197695) and is associated by the community with ZLoader [1 (https://urlhaus.abuse.ch/host/pornotublovers.com/), 2 (https://otx.alienvault.com/pulse/6114e84021bab5e48dd64903)]. The email address `neo@kosai-city[.]com` was used to register this domain and a number of others, as detailed in the full report.

Conclusion

The attack chain analyzed in this research shows how the complexity of the attack has grown in order to reach a higher level of stealthiness. The first stage dropper has been changed from the classic malicious document to a stealthy, signed MSI payload. It uses backdoored binaries and a series of LOLBAS to impair defenses and proxy the execution of their payloads.

This is the first time we have observed this attack chain in a ZLoader campaign. At the time of writing, we have no evidence that the delivery chain has been implemented by a specific affiliate or if it was provided by the main operator. SentinelLabs continues to monitor this threat in order to track further activity.

Indicators of Compromise

For a full list of IoCS see the full report.

Read the Full Report

Read the Full Report
(https://assets.sentinelone.com/sentinellabs/SentinelLabs-Zloader)

BANKING MALWARE (HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/BANKING-MALWARE/)

ZLOADER (HTTPS://WWW.SENTINELONE.COM/BLOG/TAG/ZLOADER/)

SHARE

Facebook Twitter LinkedIn Reddit Mail

ANTONIO PIROZZI (https://www.sentinelone.com/blog/author/antoniop/)

Antonio currently holds the position of Sr. Threat Intelligence Researcher at SentinelOne, where he's mainly focused on the Eastern European cybercriminal ecosystem. His expertise includes reverse engineering, malware evasion, malware phylogeny analysis.

(https://github.com/antonio-s1)

PREV

‹ **EGoManiac | An Unscrupulous Turkish-Nexus Threat Actor** (https://www.sentinelone.com/labs/egomaniac-an-unscrupulous-turkish-nexus-threat-actor/)

NEXT

CVE-2021-3437 | HP OMEN Gaming Hub Privilege Escalation Bug Hits Millions of Gaming Devices (https://www.sentinelone.com/labs/cve-2021-3437-hp-omen-gaming-hub-privilege-escalation-bug-hits-millions-of-gaming-devices/) ›

RELATED POSTS

Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare (https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/)

AUGUST 23 2021

Conti Unpacked | Understanding Ransomware Development As a Response to Detection (https://www.sentinelone.com/labs/conti-unpacked-understanding-ransomware-development-as-a-response-to-detection/)

JULY 08 2021

Evasive Maneuvers | Massive IcedID Campaign Aims For Stealth with Benign Macros (https://www.sentinelone.com/labs/evasive-maneuvers-massive-icedid-campaign-aims-for-stealth-with-benign-macros/)

JUNE 24 2021

Search ...

SIGN UP

Get notified when we post new content.

Business Email >

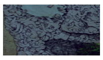
By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Policy (/legal/privacy-policy/). SentinelOne will not sell, trade, lease, or rent your personal data to third parties.

RECENT POSTS

(https://www.sentinelone.com/labs/cve-2021-3437-hp-omen-gaming-hub-privilege-escalation-bug-hits-millions-of-gaming-devices/)

CVE-2021-3437 | HP OMEN Gaming Hub Privilege Escalation Bug Hits Millions of Gaming Devices (https://www.sentinelone.com/labs/cve-2021-3437-hp-omen-gaming-hub-privilege-escalation-bug-hits-millions-of-gaming-devices/)

📅 September 14, 2021


(https://www.sentinelone.com/labs/egomaniac-an-unscrupulous-turkish-nexus-threat-actor/)

EGoManiac | An Unscrupulous Turkish-Nexus Threat Actor (https://www.sentinelone.com/labs/egomaniac-an-unscrupulous-turkish-nexus-threat-actor/)

📅 September 8, 2021

(https://www.sentinelone.com/labs/6-pro-tricks-for-rapid-macos-malware-triage-with-radare2/)

6 Pro Tricks for Rapid macOS Malware Triage with Radare2 (https://www.sentinelone.com/labs/6-pro-tricks-for-rapid-macos-malware-triage-with-radare2/)

📅 August 30, 2021

LABS CATEGORIES

Crimeware (https://www.sentinelone.com/labs/category/crimeware/)

Security Research (https://www.sentinelone.com/labs/category/security-research/)

Security & Intelligence (https://www.sentinelone.com/labs/category/security-intelligence/)

Advanced Persistent Threat (https://www.sentinelone.com/labs/category/advanced-persistent-threat/)

Adversary (https://www.sentinelone.com/labs/category/adversary/)

SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

LATEST TWEET

RT : Ukraine be like •

○

RECENT POSTS

SEPTEMBER 14, 2021

SEPTEMBER 8, 2021

AUGUST 30, 2021

SIGN UP

Get notified when we post new content.

Business Email

>

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne . SentinelOne will not sell, trade, lease, or rent your personal data to third parties.

Twitter

LinkedIn