STRRAT, ZLoader, and HoneyGain

October 19, 2021

Cisco Umbrella
Cybersecurity Threat Spotlight:
RATs, Loaders, and Unwanted Applications
Read the Article

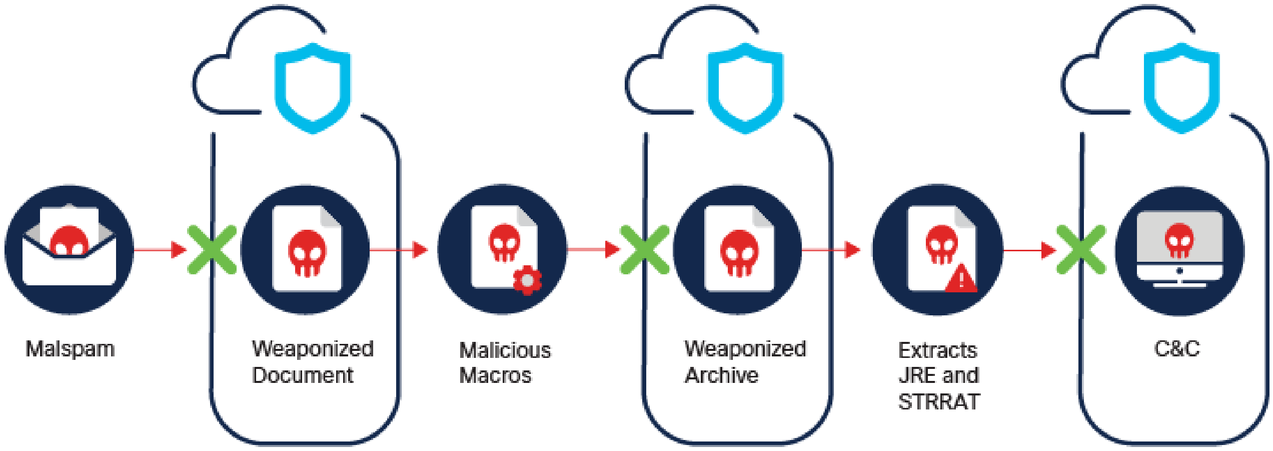
Cybersecurity Awareness Month may be in full swing, but that doesn't mean that cybercriminals have been taking a break. In fact, the opposite is true – October has seen threats like ZLoader and HoneyGain have continued to evolve. Meanwhile, STRRAT has wreaked havoc by enabling bad actors to steal credentials and install additional malware.

In today's Threat Spotlight blog, we break these threats down for you and walk through which Cisco Secure products can help protect your network. If you want to learn more about these threats, register for our on-demand webinar today!

Threat Name: STRRAT

Threat Type: RAT

Delivery and Exfiltration:



STRRAT Attack Chain

Description: STRRAT is a Java-based Remote Access Tool (RAT) that does not require a pre-installed Java Runtime Environment (JRE). It is mainly distributed through malicious spam (malspam) campaigns. The malware installs RDPWrap, steals credentials, logs keystrokes, and remotely controls Windows systems. It also contains a ransomware module.

STRRAT Spotlight: STRRAT campaigns utilize malspam as a means of initial access. If a victim opens a weaponized email attachment and enables macros within the document on a vulnerable Windows host, the macro code downloads a zip archive containing a JRE, an encrypted and obfuscated .jar file, and a script to run STRRAT using the JRE from the zip archive. The RAT focuses on stealing passwords via keylogging, as well as stored web browser and email client credentials. It supports the following browsers and email clients:

- Firefox
- Internet Explorer
- Chrome
- Foxmail
- Outlook
- Thunderbird

STRRAT also installs RDPWrap, an open source tool that enables Remote Desktop support on Windows. What’s more, STRRAT contains a ransomware module. Features and commands it supports are similar to other RATs, including the ability to download and execute additional malware.

Target Geolocations: Austria, Canada, Germany, Spain, UK, USA
Target Data: User Credentials, Browser Data, Sensitive Information
Target Businesses: Any
Exploits: N/A

Mitre Att&ck for STRAAT
Initial Access: Malspam
Persistence: Registry Run Keys / Startup Folder, Scheduled Task/Job

Execution: Scheduled Task/Job
Evasion: Obfuscated Files or Information
Collection: Automated Collection, Keylogging
Command and Control: Application Layer Protocol: Web Protocol
Exfiltration: Exfiltration Over Command and Control Channel

IOCs

Domains:
lauzon-ent[.]com
jbfrost[.]liveidgerowner[.]duckdns[.]org
adamridley.co[.]uk
alfredoscafeltd.co[.]uk
bentlyconstbuild.co[.]uk
buildersworlinc.co[.]uk
fillinaresortsltd.co[.]uk
gossyexperience.co[.]uk
jeffersonsandc.co[.]uk
jpfletcherconsultancy.co[.]uk
metroscaffingltg.co[.]uk
pg-finacesolutions.co[.]uk
playerscircleinc.co[.]uk
sivospremiumclub.co[.]uk
tg-cranedinc.co[.]uk
tk-consultancyltd.co[.]uk
westcoasttrustedtaxis.co[.]uk
zincocorporation.co[.]uk
wshsoft[.]company

IPs:
54.202.26[.]55
104.248.53[.]108
37.0.8[.]76

Additional Information:
STRRAT-Crimson
InfoSec Handlers Diary Blog

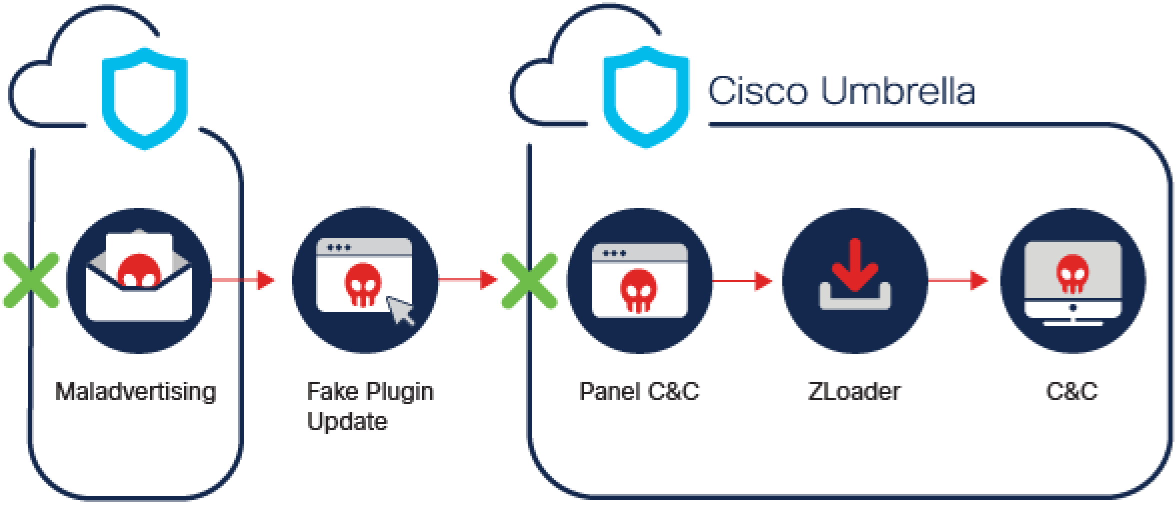
Which Cisco Products Can Block:
AMP
CWS
Network Security
Secure Network Analytics
Secure Cloud Analytics

Threat Grid
Umbrella
WSA

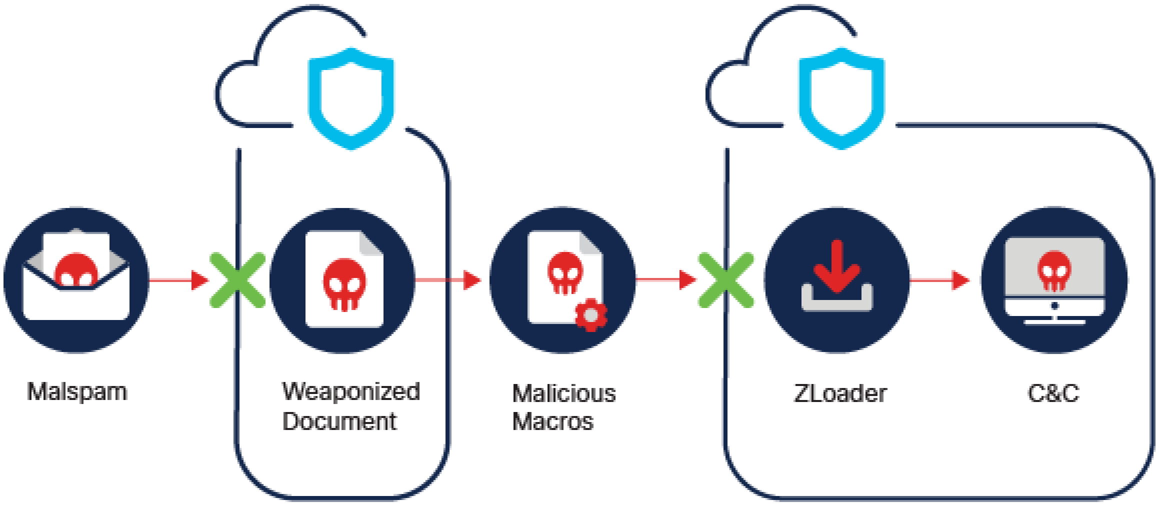
Threat Name: ZLoader (Terdot or Zbot)

Threat Type: Loader

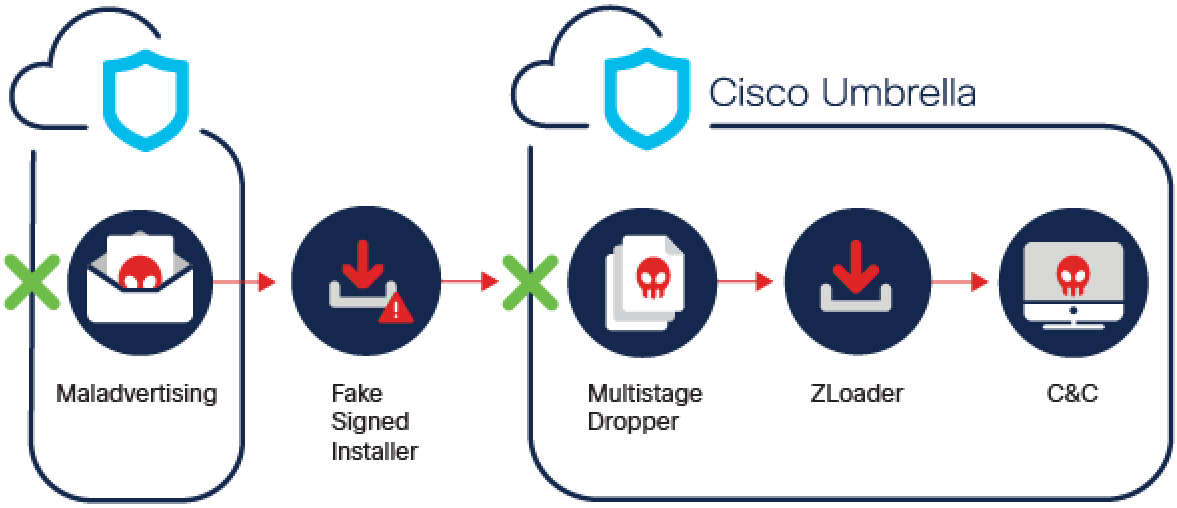
Delivery and Exfiltration: The ZLoader attack utilizes three methods of infection.



ZLoader Attack Chain no. 1



ZLoader Attack Chain no. 2



ZLoader Attack Chain no. 3

Description: ZLoader (also known as Terdot and Zbot) is a banking trojan that was first observed in 2016. It is still under active development and many versions have appeared since December 2019. It acts as a backdoor to infected systems and has the ability to download additional malware. It also implements web injection to steal cookies, passwords, and sensitive information. ZLoader targets users of financial institutions and has been used to deliver ransomware from Egregor and Ryuk families.

ZLoader Spotlight: Recent Zloader campaigns used multiple initial attack vectors. Among these are the Malsmoke malvertising campaign, phishing campaigns with malspam, and a malvertising campaign abusing advertisements published through Google Adwords. A recent evolution of the infection chain includes dynamic agent creation to download malicious payloads from a remote server. The malware can disable Windows Defender and relies on system binaries and scripts (living-off-the-land, or LOLBAS) in order to evade detection. ZLoader leverages process injection to contact its command and control server using a Domain Generation Algorithm (DGA). Once it identifies a responding domain, optional modules and a possible update to ZLoader is downloaded.

Target Geolocations: Austria, Canada, Denmark, Germany, Spain, USA
Target Data: User Credentials, Browser Data, Sensitive Information
Target Businesses: Any
Exploits: N/A

Mitre Att&ck for ZLoader
Initial Access: Malspam, Malvertising, Drive-by Compromise
Persistence: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Compromise Client Software Binary
Privilege Escalation: Abuse Elevation Control Mechanism
Execution: Command and Scripting Interpreter: PowerShell
Evasion: Process Injection: Thread Execution Hijacking, Signed Binary Proxy Execution, Signed Binary Proxy Execution: Msiexec, Signed Binary Proxy Execution: Rundll32, Impair

Defenses: Disable or Modify Tools, Subvert Trust Controls: Code Signing
Collection: Man in the Browser
Command and Control: Application Layer Protocol: Web Protocols
Exfiltration: Exfiltration Over Command and Control Channel

IOCs

Domains:
landingmonster[.]online
pornguru[.]online
pornislife[.]online
heavenlygem[.]com
moviehunters[.]site
pornofilmspremium[.]com
websekir[.]com
team-viewer[.]site
zoomvideo[.]site
iqowijsdakm[.]ru
wiewjdmkfjn[.]ru
dksaoidiakjd[.]su
iweuiqjdakjd[.]su
yuidskadjna[.]su
olksmadnbdj[.]su
odsakmdfnbs[.]com
odsakjmdnhsaj[.]com
odjdnhsaj[.]com
odoishsaj[.]com

IPs:
194.58.108[.]89
195.24.66[.]70

Additional Information:
Malsmoke Malvertising Campaign
Silent Night Campaign
Google Adwords Malvertising Campaign
New Infection Technique

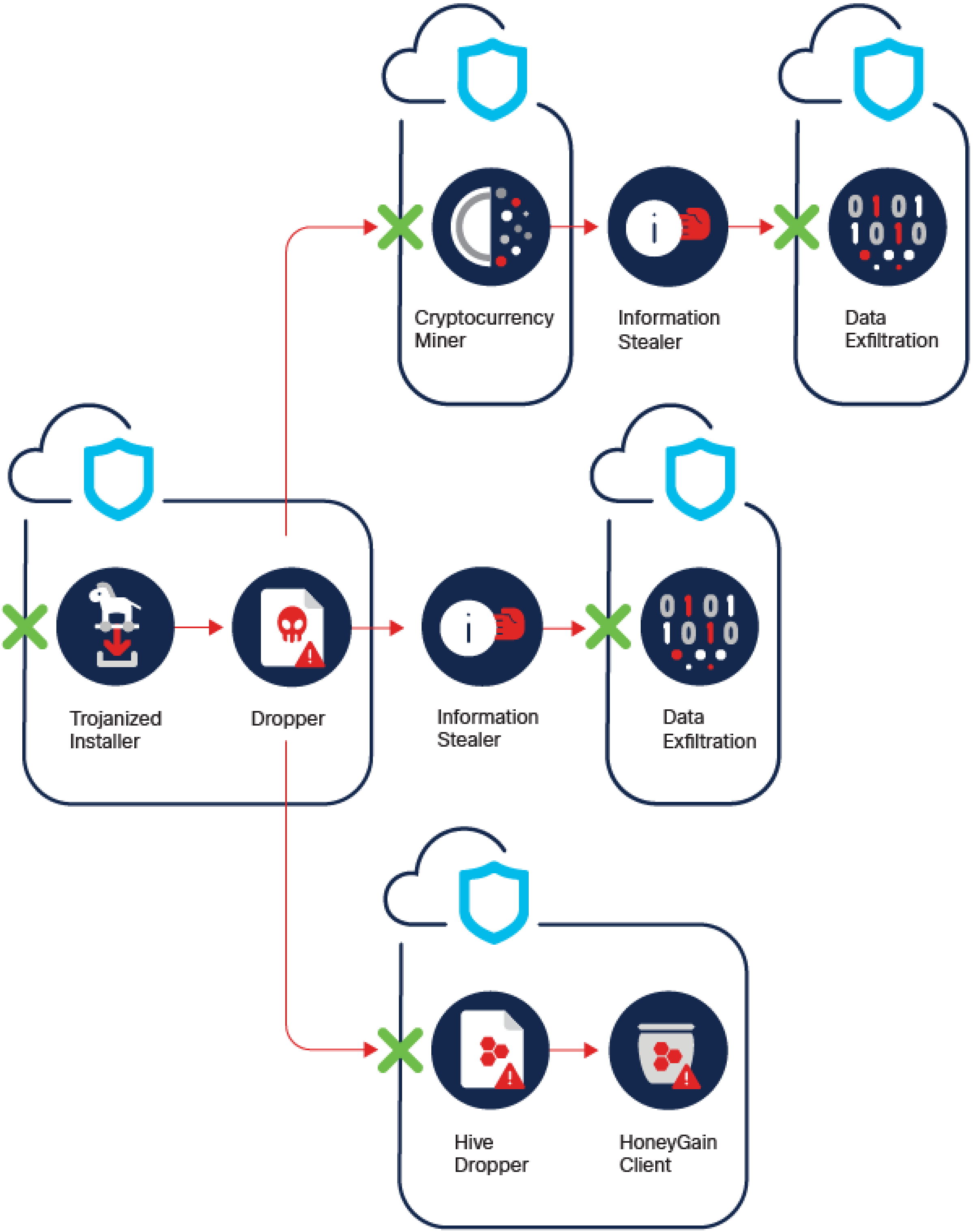
Which Cisco Products Can Block:
AMP
CWS
Network Security
Secure Network Analytics

Threat Grid
Umbrella
WSA

Threat Name: HoneyGain

Threat Type: Potentially Unwanted Application

Delivery and Exfiltration:



HoneyGain Attack Chain

Description: HoneyGain is a is legitimate software that can be used to proxy clients' connections for money. However, due to increased popularity, malicious actors started to distribute Trojanized versions of this software bundled with malicious payload. This packed malware contains a complete set of monetization methods, including a Trojanized version of the HoneyGain proxyware client, an XMRig miner, and an information stealer. The campaign continues to evolve, with the recent deployment of Nanowire client, another proxyware application with similar functionality.

HoneyGain Spotlight: A variety of different malware families are being distributed under the guise of legitimate installers for applications like HoneyGain. These trojanized installers enable adversaries to distribute threats such as RATs, information stealers, and other malware to victims who believe they are installing legitimate applications. Associated malware was also observed leveraging victims' CPU resources to mine cryptocurrency, while also monetizing their network bandwidth using proxyware applications. One of the most common techniques observed is the use of legitimate installers as decoy programs included alongside other malicious components. In these attacks, threat actors are distributing malicious executables posing as installers for legitimate proxyware applications like HoneyGain. When executed, they will typically install the legitimate application while silently installing malware.

Target Geolocations: World-Wide
Target Data: Browser Data, Sensitive Data
Target Businesses: Any
Exploits: N/A

Mitre Att&ck for HoneyGain
Persistence: Scheduled Task/Job, Registry Run Keys / Startup Folder, Windows Service
Execution: Scheduled Task, Native API
Evasion: N/A
Collection: N/A
Command and Control: Application Layer Protocol: Web Protocols
Exfiltration: Exfiltration Over Command and Control Channel

IOCs

Domains:
ariesbee[.]com
bootesbee[.]com
aurigabee[.]xyz
analytics[.]honeygain[.]com
api[.]honeygain[.]com
download[.]honeygain[.]com
www[.]xsvpn[.]cf
terminist-journal[.]000webhostapp[.]com
r[.]honeygain[.]money

URLs:
hxxps://www.dropbox[.]com/s/vhpmmwns1k9wh33/Honeygain.zip?dl=1
hxxps://www.dropbox[.]com/s/rfbrftww47y0edv/nanowire.exe?dl=1
hxxps://www.dropbox[.]com/s/7hy2ausr3rouflp/nanowire.toml?dl=1
hxxps://www.dropbox[.]com/s/gq3tt6iawri6m3w/user.config?dl=1
hxxps://www.dropbox[.]com/s/puz02l0l7a4wjmt/beehive.txt?dl=1
hxxps://www.dropbox[.]com/s/gp7s712krr67kcx/MinerDownloader-1-23-21.txt?dl=1
hxxps://docs.google[.]com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download
hxxps://www.dropbox[.]com/s/zhp1b06imehwylq/Synaptics.rar?dl=1
hxxps://www.dropbox[.]com/s/ve1i21h0ubslnkr/xmrig2.txt?dl=1
hxxps://www.dropbox[.]com/s/h5lge8h8rhw93rh/Stealer%201-23-21.txt?dl=1
hxxps://www.dropbox[.]com/s/8jyj3a5vw1bwot9/ChromePass.txt?dl=1
hxxps://www.dropbox[.]com/s/v8x3jnnx15hjz04/WebBrowserPassView.txt?dl=1
hxxps://r.honeygain[.]money/SAMIBDC7
hxxps://iplogger[.]org/2jbNj6
hxxps://iplogger[.]org/2azxA5
hxxp://www.xsvpn[.]cf/ssr-download/readme.md

Stealer Exfiltration URL:
hxxps://terminist-journal.000webhostapp[.]com/donkeydick.php

Additional Information:
HoneyGain

Which Cisco Products Can Block:
AMP
CWS
Network Security
Secure Network Analytics
Secure Cloud Analytics
Threat Grid
Umbrella
WSA

Want to Learn More About This Month’s Leading Cyberattacks?

Register for our on-demand webinar today to learn more about how these threats operate and what you can do to protect your network against them.