Backdoors, RATs, Loaders evasion techniques

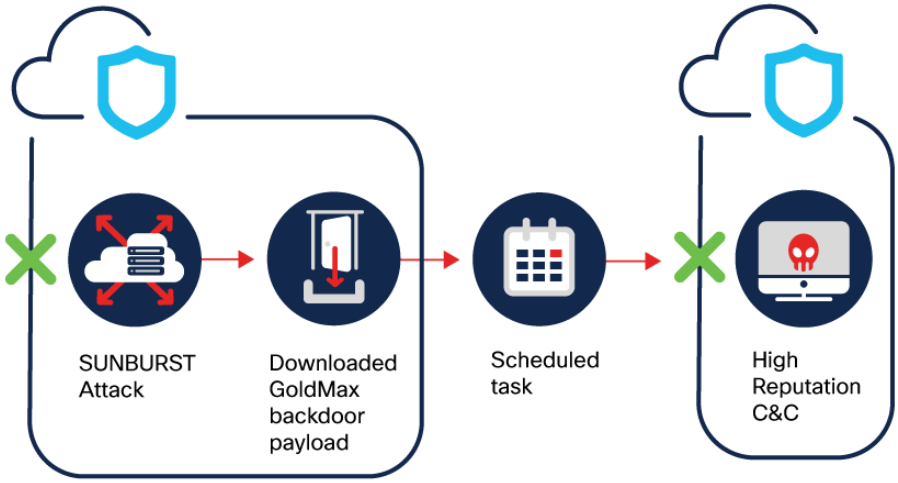
umbrella.cisco.com/blog/cybersecurity-threat-spotlight-backdoors-rats-loaders-evasion-techniques

June 1, 2021

In this second edition of the Cybersecurity Threat Spotlight, we're examining the most important current threats including a backdoor threat, a remote access trojan (RAT), and a loader. Obfuscation, encryption, weaponization of normally benign files, and remote (frequently C2) execution continue to be primary techniques in ongoing use.

Threat Name: GoldMax

Threat Type: Backdoor
Actor: NOBELIUM
https://attack.mitre.org/groups/G0118/
Delivery and Exfiltration:



Cisco Umbrella detects SUNBURST domains, domains hosting GoldMax payload, and C&C servers.
Description: GoldMax (also known as SUNSHUTTLE) is a post-exploitation malware currently used as part of a SUNBURST attack. SUNBURST uses multiple techniques to obfuscate its actions and evade detection. GoldMax persists on systems as a scheduled task, impersonating systems management software.

GoldMax Spotlight: Written in Go, GoldMax acts as a command-and-control backdoor for the actor. The malware writes an encrypted configuration file to disk, where the file name and AES-256 cipher keys are unique per implant, and based on environmental variables and information about the network where it is running. The C2 can send commands to be launched for various operations, including native OS commands, via pseudo-randomly generated cookies. The hardcoded cookies are unique to each implant, mapping to victims and operations on the actor side. GoldMax is equipped with a decoy network traffic generation feature that allows it to surround its malicious network traffic with seemingly benign traffic.

Target geolocations: North America, Europe
Target data: Any
Target businesses: Government, public entities, private entities

Mitre Att&ck, GoldMax
Initial access: Supply chain compromise
Persistence: Scheduled task
Execution: Command and scripting interpreter: windows command shell
Evasion: Deobfuscate/decode files or information, obfuscated files or information: software packing, indirect command execution, masquerade task or service, system checks
Collection: N/A
Command and Control: Encrypted channel: symmetric cryptography, data encoding, data obfuscation, ingress tool transfer, web protocols
Exfiltration: exfiltration over C2 channel

IOCs:
Domains:
srfnetwork[.]org
reyweb[.]com
onetechcompany[.]com
IPs:
185.225.69[.]69
SHA-256 Hashes:
70d93035b0693b0e4ef65eb7f8529e6385d698759cc5b8666a394b2136cc06eb
0e1f9d4d0884c68ec25dec355140ea1bab434f5ea0f86f2aade34178ff3a7d91
247a733048b6d5361162957f53910ad6653cdef128eb5c87c46f14e7e3e46983
F28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c
611458206837560511cb007ab5eeb57047025c2edc0643184561a6bf451e8c2c
B9a2c986b6ad1eb4cfb0303baede906936fe96396f3cf490b0984a4798d741d8
bbd16685917b9b35c7480d5711193c1cd0e4e7ccb0f2bf1fd584c0aebca5ae4c

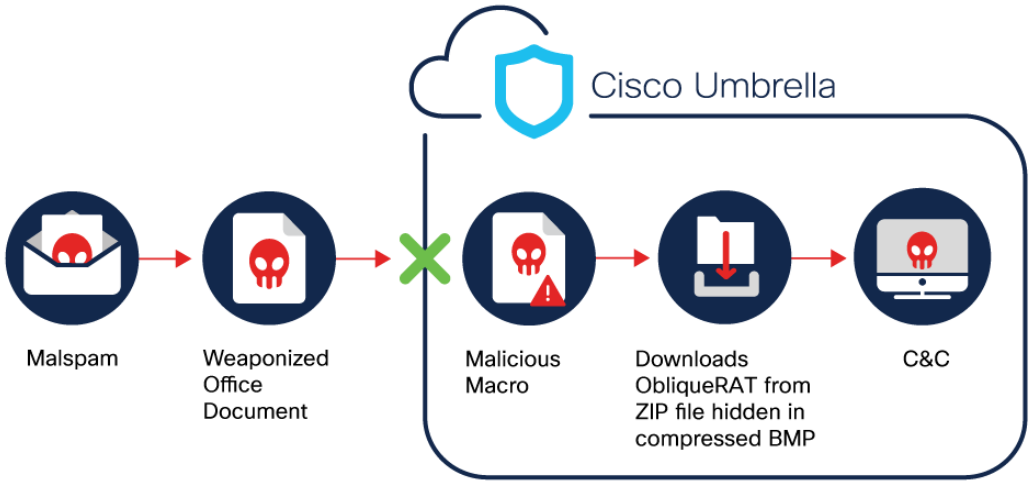
Additional Information:
https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html

Which Cisco products can block GoldMax:

- Cisco Secure Endpoint (AMP for Endpoints)
- Cisco Cloud Web Security (CWS)
- Cisco Network Security
- Cisco Secure Network Analytics
- Cisco Secure Cloud Analytics
- Cisco Secure Web Appliance
- Cisco Threat Grid
- Cisco Umbrella

Threat Name: ObliqueRAT

Threat Type: Remote Access Trojan
Actor: Transparent Tribe
Delivery and Exfiltration:



Cisco Umbrella detects domains hosting malicious documents, malicious Zip files, and C&C servers.
Description: Oblique is a popular Remote Access Trojan, currently being used to take remote control of infected systems and steal data. The malware has the following capabilities: get the running process on the system, get the drives, directories, and files on the system, get the host names, user IDs, capture screenshots, get the data from C2 server, using custom ports to connect to C2 server.

ObliqueRAT Spotlight: ObliqueRAT is related to CrimsonRAT, sharing the same malware documents and macros, but using its macro code to download its malicious payload from actor-controlled websites. The malicious payload appears to be benign BMP image files. These files contain a ZIP, which holds the ObliqueRAT payload. Once downloaded and extracted, the file is renamed with a .pif file extension. Persistence is achieved by creating a shortcut with a .URL file extension in the infected user's Startup.

Target geolocations: South Asia
Target data: Credentials from web browsers, data from removable media, local email collection
Target businesses: Any

Mitre Att&ck, ObliqueRAT
Initial access: Phishing
Persistence: Registry run keys / startup folder
Execution: Scheduled task/job
Evasion: Impair defenses
Collection: File and directory discovery, process discovery, screen capture, security software discovery, system Information discovery, system network configuration discovery
Command and control: Data obfuscation
Exfiltration: Ingress tool transfer, exfiltration over command and control channel using non-application layer protocol

IOCs:
Domains:
larsentobro[.]com
micrsoft[.]ddns.net
URLs:
hxxp://iiaonline[.]in/DefenceLogo/theta.bmp
hxxp://iiaonline[.]in/timon.jpeg
hxxp://iiaonline[.]in/9999.jpg
hxxp://iiaonline[.]in/merj.bmp
hxxp://iiaonline[.]in/111.jpg
hxxp://iiaonline[.]in/sasha.jpg
hxxp://iiaonline[.]in/111.png
hxxp://iiaonline[.]in/camela.bmp
hxxp://larsentobro[.]com/mbda/goliath1.bmp
hxxp://larsentobro[.]com/mbda/mundkol
hxxp://drivestransfer[.]com/myfiles/Dinner%20Invitation.doc/win10/Dinner%20Invitation.doc
IPs:
185[.]183.98.182

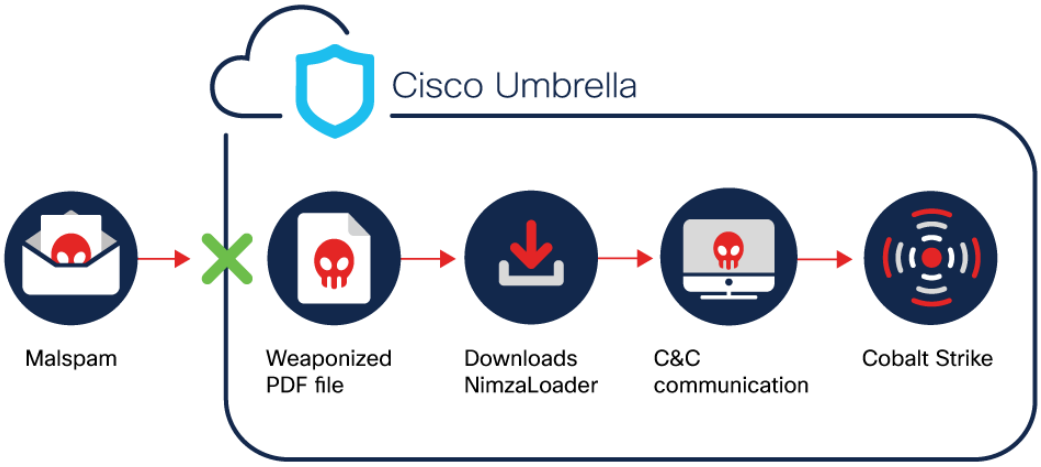
Additional Information:
https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html

Which Cisco products can block ObliqueRAT:

- Cisco Secure Endpoint
- Cloud Web Security
- Cisco Secure Email
- Cisco Secure Firewall/Secure IPS
- Cisco Secure Malware Analytics
- Cisco Umbrella
- Cisco Secure Web Appliance

Threat Name: NimzaLoader

Threat Type: Loader
Actor: TA800
Delivery and Exfiltration:



Cisco Umbrella detects domains hosting malicious documents, malicious NimzaLoader payload, C&C servers and Cobalt Strike communications.
Description: NimzaLoader is part of a malware family used by the TA800 threat group to gain a foothold in compromised enterprise networks. This threat group previously used BazaLoader before switching to the new NimzaLoader in February 2021.

NimzaLoader Spotlight: NimzaLoader is written in the Nim programming language in an attempt to avoid detection. JSON files are used for data storage, memory management, and C&C communication and it does not use a domain generation algorithm. Second-stage payload is most commonly Cobalt Strike.

Exploitation begins with phishing emails to victims containing personalized details that can be found on social networking sites such as LinkedIn. The emails contain a link, labeled as 'PDF-preview' that leads to a NimzaLoader download webpage.

NimzaLoader makes use of cmd.exe and powershell.exe to inject shellcode into a process on Windows systems. It utilizes a heartbeat mechanism to update expiration dates of the malware in memory and encodes other data in a JSON object.

Target geolocations: Any
Target data: Any
Target businesses: Any
Exploits: N/A

Mitre Att&ck, NimzaLoader
Initial access: Spearphishing attachment, spearphishing link
Persistence: Registry run keys / startup folder, startup items, hooking
Evasion: Deobfuscate / decode files or information, masquerading, obfuscated files or information, process doppelganging, process hollowing, process injection
Collection: Account discovery, application window discovery, file and directory discovery, process discovery, query registry, remote system discovery, security software discovery,

system information discovery, system time discovery, system owner / user discovery
Exfiltration: Commonly used port, data encrypted, remote file copy, standard application layer protocol, standard cryptographic protocol, standard non-application layer protocol

IOCs:
Domains:
centralbancshares[.]com
gariloy[.]com
liqui-technik[.]com
SHA-256 Hashes:
540c91d46a1aa2bb306f9cc15b93bdab6c4784047d64b95561cf2759368d3d1d

Additional Information:
https://www.technadu.com/ta800-group-using-new-initial-access-tool-nimzaloader/253752/

Which Cisco products can block NimzaLoader:

- Cisco Secure Endpoint
- Cloud Web Security
- Cisco Secure Email
- Cisco Secure Firewall/Secure IPS
- Cisco Secure Malware Analytics
- Cisco Umbrella
- Cisco Secure Web Appliance