MITRE ENGENUITY | Center for Threat Informed Defense

Intrusion Analysis Report

Remote Access Tool Detected, Proxy Execution by Legitimate Management Tools, Second-Stage Malware C2 Connections, and Eventual Ransomware Likely

Date of Report :

March 20, 2023

Executive Summary

We assess with moderate confidence that Water Minyades is the threat actor responsible for this intrusion and intends to deploy ransomware. Syncro RAT is often leveraged by Water Minyades as a second-stage loader deployed by Batloader malware as the primary means of persistence during an intrusion. Generally, Syncro is deployed alongside other legitimate tools, such as Nsudo, Gpg4win, NirCmd, PowerShell, MsiExec.exe, and Mshta.exe, which are used for proxy execution and privilege escalation. After gaining persistence through Syncro RAT, it is likely that Water Minyades will leverage second-stage malware, such as Cobalt Strike, for C2 and exfiltration purposes, as well as attempt to exploit the domain controller to push the ransomware module.

Key Points

- In the intrusion chain, Syncro RAT falls under persistence and C2. The IR team should look for activity targeting the domain controller, as well as legitimate system management and file execution tools used for privilege escalation and proxy execution, as well as C2 connections from second-stage malware such as Cobalt Strike.
- Key Syncro RAT capabilities include the ability to terminal with SYSTEM privileges, deploy additional backdoors, gain remote desktop and full file system access, and exfiltrate files.
- Water Minyades is the threat actor likely responsible for the intrusion due to the use of a watering hole as an initial intrusion vector; however, Luna Moth and MuddyWater also are associated with the tool. If our attribution assessment proved incorrect, data theft and/or extortion is likely.
- Syncro Rat is deployed through phishing or by the Batloader malware as a post-compromise tool. Water Minyades has used Syncro in operations that ultimately led to the deployment of ransomware.

Indicator Analysis

We assess with moderate confidence that Water Minyades is the threat actor behind this attack. The adversary's capabilities, infrastructure, and TTPs align most closely with the observed activity. The next step in the intrusion chain is likely lateral movement to the domain controller to facilitate ransomware deployment. At this early stage we cannot completely rule out that Luna Moth or MuddyWater could also be responsible for the intrusion as both intrusion groups have leveraged Syncro in the past.

Water Minyades TTPs likely to be used during a campaign include the following:

- In previous intrusions, the threat actor conducted SEO Poisoning to trick users into downloading malicious .MSI files that masquerade as legitimate software installers and deliver the Batloader malware (T1204, T1608.006, T1036.005).

- In previous intrusions, the threat actor conducted host discovery and checked for artifacts such as user, computer name, and if domain joined (T1033, T1482).

- The threat actor will likely seek to establish additional C2 connections, maintain persistence, and escalate privileges by installing additional malware and abusing legitimate tools. Batloader uses a modular approach wherein the first-stage payload is usually an MSI file bundled with custom action scripts, which download legitimate tools and malware payloads (T1105, T1218).

- Batloader has been observed using legitimate tools such as:
    - Nsudo – run processes with elevated privileges
    - Gpg4win – decrypt next-stage payloads downloaded by Batloader
    - NirCmd – command-line
    - PowerShell – run malicious powershell scripts
    - MsiExec.exe – run MSI files with malicious custom action scripts
    - Mshta.exe, and others – execute malicious code appended to PE files.

- On enterprise environments, Batloader has been observed dropping malware payloads such as Cobalt Strike Beacon but may also deploy other families, such as Bumbleloader or Qakbot. The payloads are usually hyperinflated and encrypted to evade defenses (T1105, T1027). These payloads can be used for follow-on actions, such as credential and information theft (TA0006). In previous intrusions, the threat actor has used a remote management tool and Cobalt Strike Beacon to facilitate ransomware deployment.

- The threat actors may move laterally by abusing legitimate file sharing services to host malware payloads (T1080).

- The threat actors will likely seek to evade defenses by hyperinflating MSI file sizes to avoid AV detection, obfuscating scripts connected to the C2 servers, and stopping services related to security (T1027.001, T1001, T1562.001).

Potential Alternative Threat Actors

Luna Moth also leverages Syncro RAT during its operations. In past intrusions, this threat actor achieves persistence by using multiple legitimate remote access tools such as Atera, Splashtop, Syncro, and AnyDesk, to reinstall a RAT if it is removed. Additional tools used by the group include commercially available tools such as SoftPerfect Network Scanner, SharpShares, and RClone and are stored under false names masquerading as legitimate binaries (T1036.005). These tools, in combination with the RATs, allow the threat actor to conduct reconnaissance, move laterally, and exfiltrate data. This threat actor's end goal is likely data theft and extortion.

MuddyWater is also associated with the use of Syncro RAT by at least one security vendor. In a past intrusion with a different legitimate RAT, this threat actor established persistence using a start-up folder, evaded defenses using LOLbins, accessed credentials using Browser64.exe, and blended their C2 traffic using web protocols (T1547.001, T1218, T1555, T1437.001). This threat actors' end goal is likely espionage and data theft.

MITRE ATT&CK Table (based on v12)
TTPs Likely to Be in the Network

ATTRIBUTION	TACTICS	TECHNIQUE	SUBTECHNIQUE	PROCEDURE	D3FEND	DEPLOYED CONTROL
Water Minyades	Resource Development	T1608: Stage Capabilities	T1608.006: Stage Capabilities: SEO Poisoning	Water Minyades uses malvertising to direct users to Batloader distribution sites.	N/A	N/A
Water Minyades	Execution	T1204: User Execution	N/A	Water Minyades relies on the user to install a malicious file.	LINK	User Training
Water Minyades	Discovery	T1033: System Owner/ User Discovery	N/A	Batloader fingerprints the host to determine if it is a legitimate victim. It also checks for user and computer name.	LINK	N/A
Water Minyades		T1482: Domain Trust Discovery	N/A	Batloader checks if the host is domain joined.	N/A	N/A
Water Minyades	Command and Control	T1105: Ingress Tool Transfer	N/A	Batloader is a modular malware that later installs legitimate system management and file execution tools and malware payloads.	LINK	Monitor File Creation Processes
Water Minyades		T1001: Data Obfuscation	N/A	Batloader obfuscates scripts connected to its C2.	LINK	Network Intrusion Prevention

ATTRIBUTION	TACTICS	TECHNIQUE	SUBTECH-NIQUE	PROCEDURE	D3FEND	DEPLOYED CONTROL
Water Minyades	Defense Evasion	T1027: Obfuscated Files or Information	N/A	Batloader downloads additional malware payloads, which are often hyperinflated and encrypted.	LINK	Antivirus
Water Minyades		T1027: Obfuscated Files or Information	T1027.001 Obfuscated Files or Information: Binary Padding	Water Minyades is known for deploying payloads, such as the Batloader malware, with large file size to evade sandbox analysis and antivirus engines' file size limits.	LINK	
Water Minyades		T1218: System Binary Proxy Execution	N/A	Batloader bypasses process and/or signature-based defenses by abusing legitimate tools.	LINK	N/A
Water Minyades		T1562: Impair Defenses:	T1562.001: Impair Defenses: Disable or Modify Tools	Batloader executes open-sourced scripts that attempt to stop services related to security software, such as Windows Defender.	LINK	Restricted File, Directory, and Registry Permissions
Water Minyades		T1036: Masquerading:	T1036.005: Masquerading: Match Legitimate Name or Location	Water Minyades tricks users into downloading Batloader from legitimate-looking websites and abuses MSI file's legitimate digital signatures to package the malware. The malicious file may also be a VHD, VHDX, or JavaScript file.	LINK	User Training
Water Minyades	Lateral Movement	T1080: Taint Shared Content	N/A	Batloader abuses legitimate file sharing services to host malware payloads.	LINK	Restricted File and Directory Permissions
Water Minyades	Credential Access	N/A	N/A	Water Minyades has used second-stage malware such as Cobalt Strike to steal credentials.	N/A	N/A
Water Minyades	Impact	T1486 Data Encrypted for Impact	N/A	Water Minyades generally attempts to facilitate ransomware using Syncro.	N/A	Data Backup

MITRE ATT&CK Table (based on v12) TTPs Observed in the Intrusion

TATICS	TECHNIQUE	SUBTECHNIQUE	PROCEDURE	D3FEND
Resource Development	T1608: Stage Capabilities	T1608.006: Stage Capabilities: SEO Poisoning	Several users visited a seemingly legitimate site set up by the threat actor.	N/A
Execution	T1204: User Execution	N/A	The users downloaded a malicious file that installed Syncro.	LINK
Defense Evasion	T1036: Masquerading	T1036.005: Masquerading: Match Legitimate Name or Location	The malicious file masqueraded as a legitimate installer.	LINK

Indicators of Compromise for Hunting Malware

ATTRIBUTION	MALICIOUS TOOL NAME	HASH TYPE	FILE HASH	ASSOCIATED FILE HASH	BRIEF DESCRIPTION	MALWARE ANALYSIS REPORT (HYPERLINK, OR N/A)	FIRST REPORTED	LAST REPORTED
Water Minyades	Batloader	SHA256	61e0926120f493d5edf3a50842b04640911974ecbbc93b6b33ca20c1f981bc	N/A	Batloader file installed after User Execution.	LINK	February 6 2023	March 2023
Water Minyades	Batloader	SHA256	91730741d72584f96ccba99a09b17be6d64728673871858ea917543c1e	N/A	Batloader file installed after User Execution.	N/A	N/A	March 2023
Water Minyades	Batloader	SHA256	23373654d02cb7eace932609826cca4f82fcac67ca44b9328baba385acc00C67	2e65cfebde138e4dd816d3e8b8105e796c4eb38cfa27015938c045ee5be8331	Batloader file installed after User Execution.	LINK	March 2023	March 2023
Water Minyades	Batloader	SHA256	f8f3f22425ea72fafba5453c70c299367bd144c95e61b348d1e6dda0c469e219	2e65cfebde138e4dd816d3e8b8105e796c4eb38cfa27015938c0445ee5be8331	Batloader file installed after User Execution.	LINK	March 2023	March 2023

NETWORK

ATTRIBUTION	NETWORK ARTIFACT	DETAILS	INTRUSION PHASE	FIRST REPORTED	LAST REPORTED
Water Minyades	105105105015[.]com	Downloads the next-stage payload after initial Batloader infection	C2	October 2022	March 2023
Water Minyades	24xpixeladvertising[.]com	Downloads the next-stage payload after initial Batloader infection	C2	October 2022	March 2023
Water Minyades	clodtechnology[.]com	Downloads the next-stage payload after initial Batloader infection	C2	October 2022	March 2023
Water Minyades	cloudupdatesss[.]com	Downloads the next-stage payload after initial Batloader infection	C2	September 2022	March 2023
Luna Moth	dictumst[.]xyz		Exfiltration	March 2022	March 2023
Luna Moth	masterzohoclass[.]com		Infrastructure	March 2022	March 2023

SIGNATURES

1. Batloader

```
rule M_Hunting_Downloader_BATLOADER_1
{
meta:
author = “Mandiant”
date_created = “2021-10-28”
date_modified = “2021-10-28”
version = “1.0”
description = “Detects strings for BATLOADER sample”
md5 = “6cd13e6429148e7f076b479664084488”

strings:
$s1 = “launch.bat” ascii
$s2 = “Error writing to batch file:” ascii
$s3 = “cmd.exe” ascii
$s4 = “/C” ascii
```

$s5 = “You entered an invalid email, please enter the email that was registered on website.” ascii

condition:
uint16(0) == 0x5A4D and filesize > 4KB and filesize < 5MB and all of them
}

2. Syncro

a.title: Process Creation Using Sysnative Folder
id: 3c1b5fb0-c72f-45ba-abd1-4d4c353144ab
status: experimental
description: Detects process creation events that use the Sysnative folder (common for CobaltStrike spawns)
references:
- https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
author: Max Altgelt (Nextron Systems)
date: 2022/08/23
tags:
- attack.t1055
logsource:
category: process_creation
product: windows
detection:
sysnative:
CommandLine|startswith: ‘C:\Windows\Sysnative\’
condition: sysnative
fields:
- CommandLine
- ParentCommandLine
falsepositives:
- Unknown
level: medium

b. title: Failed Code Integrity Checks
id: 470ec5fa-7b4e-4071-b200-4c753100f49b
status: stable
description: Detects code integrity failures such as missing page hashes or corrupted drivers due unauthorized modification. This could be a sign of tampered binaries.
author: Thomas Patzke
date: 2019/12/03
modified: 2020/08/23
tags:
- attack.defense_evasion

```
    - attack.t1027.001
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID:
            - 5038
            - 6281
    condition: selection
falsepositives:
    - Disk device errors
level: low
```

PROBABILITY MATRIX

ALMOST NO CHANCE	VERY UNLIKELY	UNLIKELY	ROUGHLY EVEN CHANCE	LIKELY	VERY LIKELY	ALMOST CERTAINLY
remote	highly improbable	improbable (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

INTELLIGENCE REQUIREMENTS

- Identify and research activity targeting critical assets
- Identify and research actors targeting similar organizations

FEEDBACK

Please take a moment to provide feedback on this report by emailing EXAMPLE@companydomain.com; all comments are reviewed and used to enhance future reporting.

1. Rate the product's overall value:
    a. Very valuable
    b. Somewhat valuable
    c. Of limited value
    d. Not valuable

2. Rate the product's utility:
   a. Highly actionable
   b. Actionable
   c. Not actionable.
3. Rate the product's quality of analysis:
   a. High quality analysis
   b. Acceptable quality analysis
   c. Low quality analysis
4. Rate the product's timeliness:
   a. Very timely
   b. Timely
   c. Not timely.
5. What did you find particularly useful or lacking in the report?

DATA SOURCES

https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

https://www.mandiant.com/resources/blog/seo-poisoning-batloader-atera

https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks

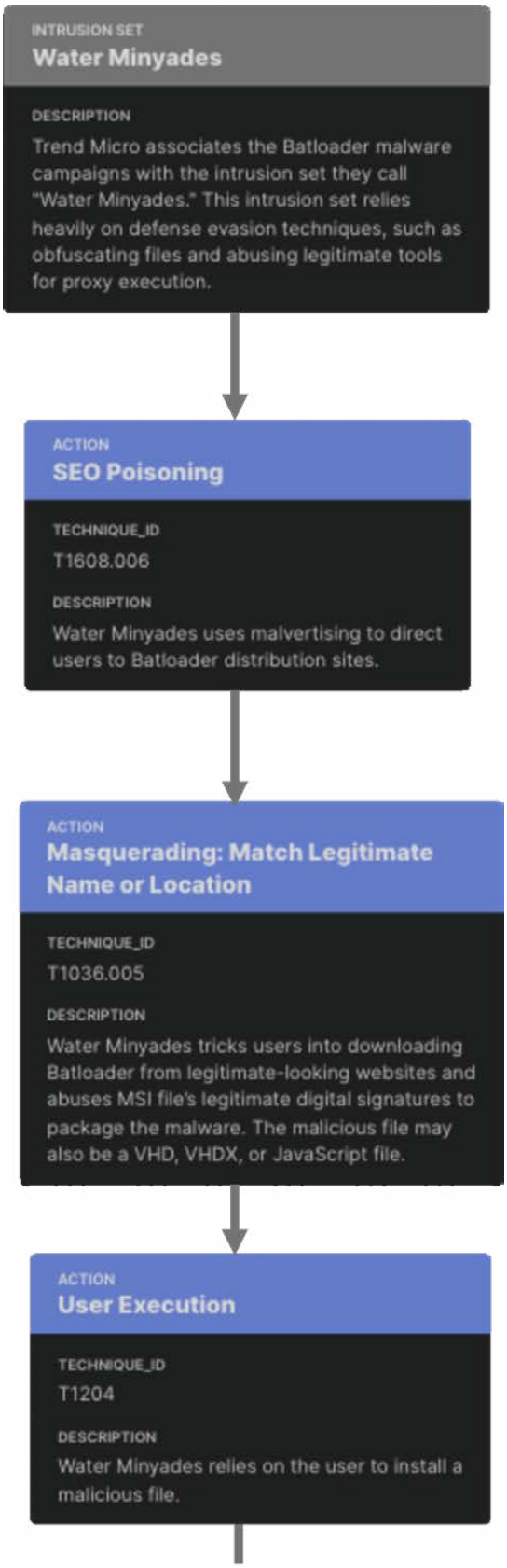
https://www.trendmicro.com/en_us/research/23/a/batloader-malware-abuses-legitimate-tools-uses-obfuscated-javasc.html

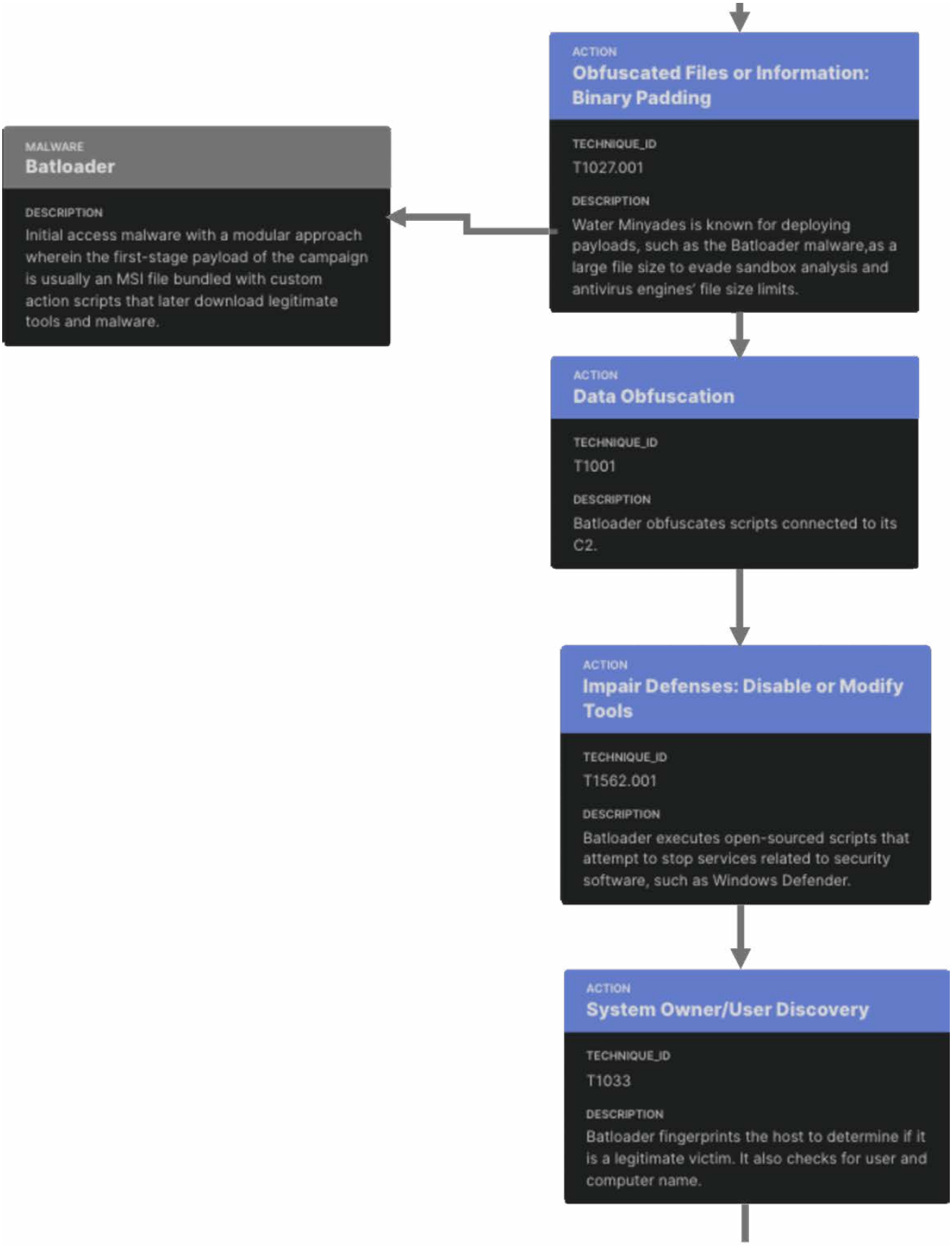
https://blog.sygnia.co/luna-moth-false-subscription-scams

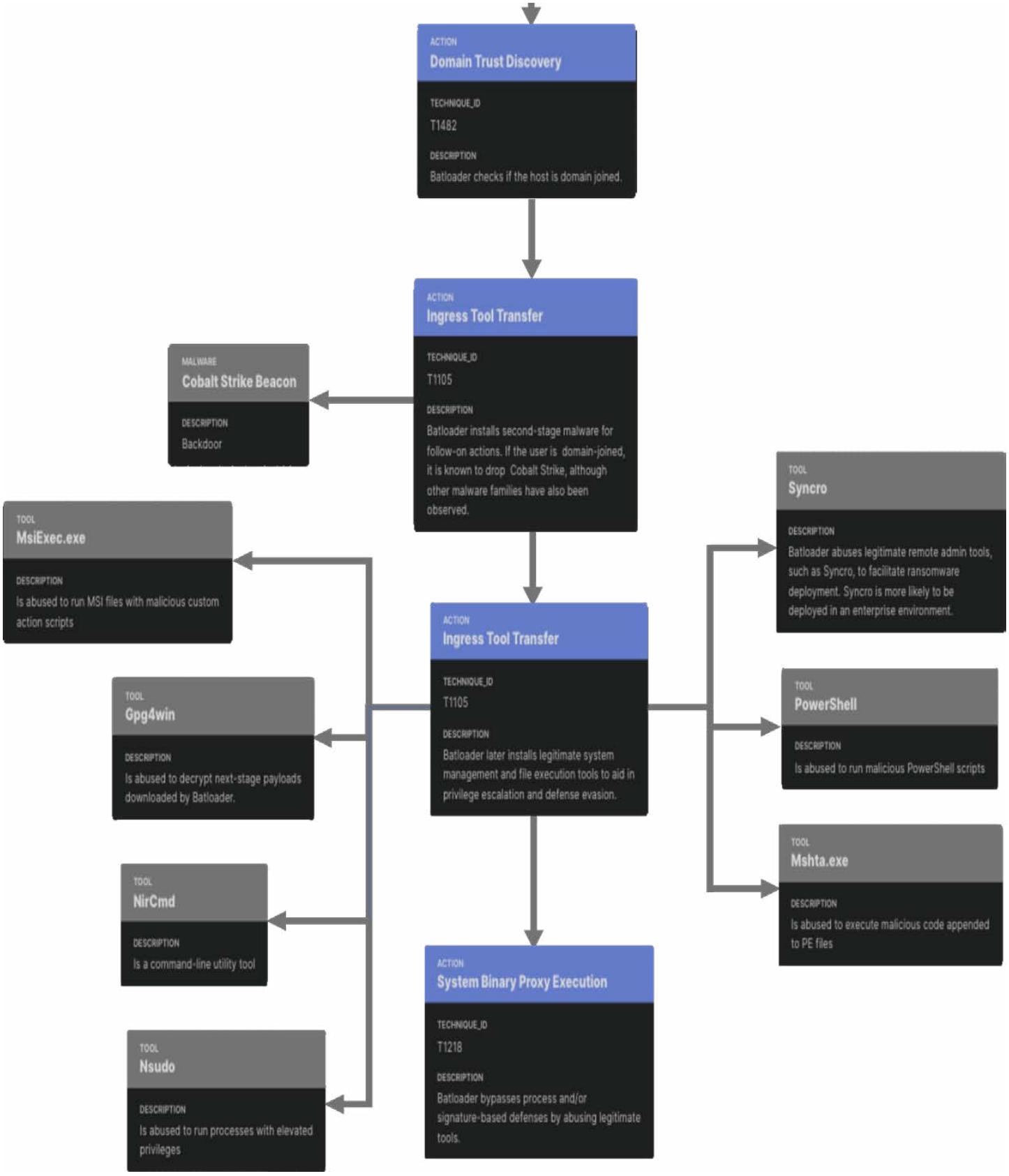
209.160.24.63- - [19/Mar/2023:18:22:16] "GET /product.screen?productId=WC-SH-A02&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 3878 "http://www.advancedinstaller1.com" " Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 349

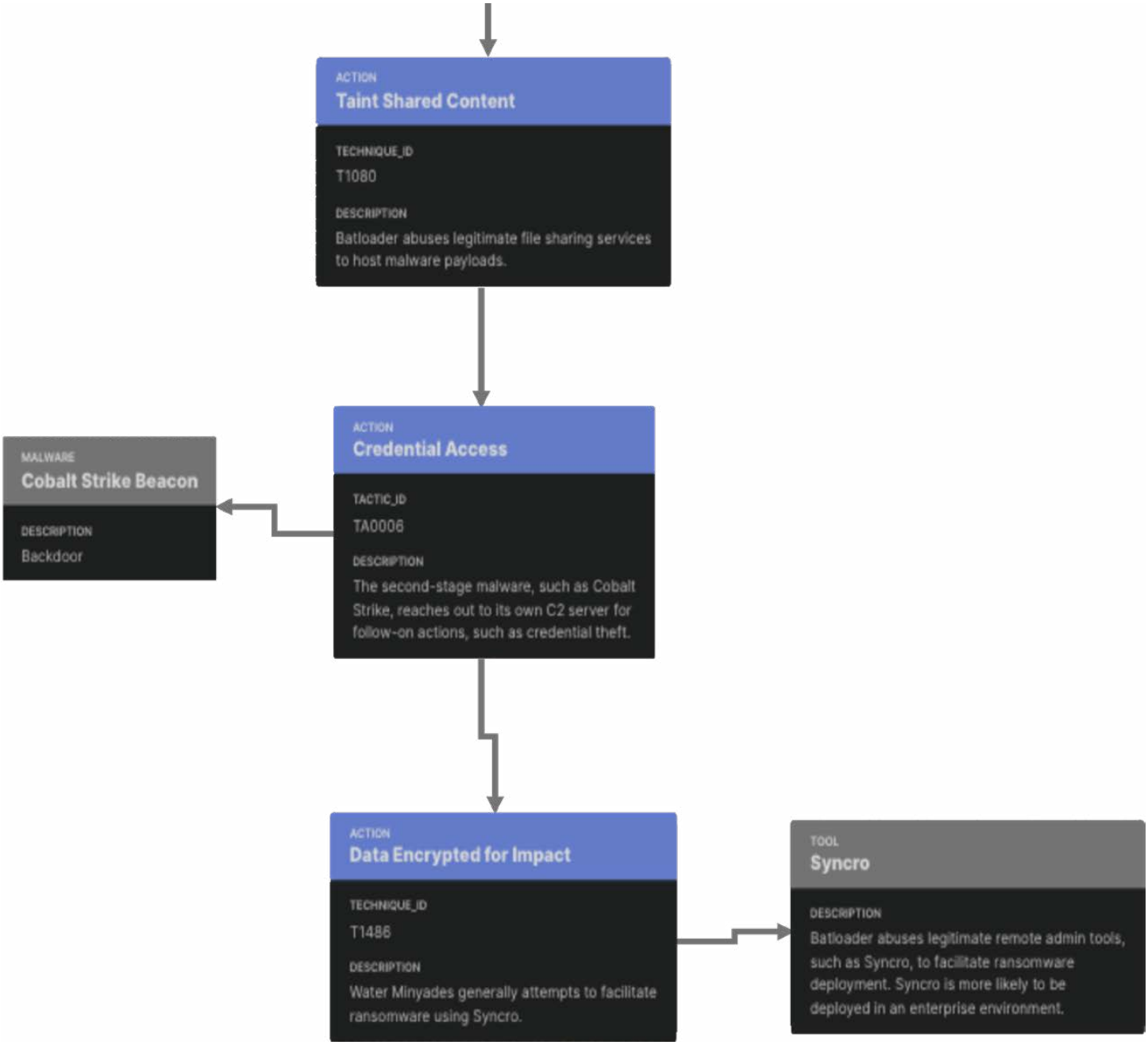
Threat Actor: Water Minyades
DEV-0569

Actor Motivation: Ransomware


INTRUSION SET
Water Minyades
DESCRIPTION
Trend Micro associates the Batloader malware campaigns with the intrusion set they call "Water Minyades." This intrusion set relies heavily on defense evasion techniques, such as obfuscating files and abusing legitimate tools for proxy execution.
ACTION
SEO Poisoning
TECHNIQUE_ID
T1608.006
DESCRIPTION
Water Minyades uses malvertising to direct users to Batloader distribution sites.
ACTION
Masquerading: Match Legitimate Name or Location
TECHNIQUE_ID
T1036.005
DESCRIPTION
Water Minyades tricks users into downloading Batloader from legitimate-looking websites and abuses MSI file's legitimate digital signatures to package the malware. The malicious file may also be a VHD, VHDX, or JavaScript file.
ACTION
User Execution
TECHNIQUE_ID
T1204
DESCRIPTION
Water Minyades relies on the user to install a malicious file.


ACTION
Obfuscated Files or Information: Binary Padding
TECHNIQUE_ID
T1027.001
DESCRIPTION
Water Minyades is known for deploying payloads, such as the Batloader malware,as a large file size to evade sandbox analysis and antivirus engines' file size limits.
MALWARE
Batloader
DESCRIPTION
Initial access malware with a modular approach wherein the first-stage payload of the campaign is usually an MSI file bundled with custom action scripts that later download legitimate tools and malware.
ACTION
Data Obfuscation
TECHNIQUE_ID
T1001
DESCRIPTION
Batloader obfuscates scripts connected to its C2.
ACTION
Impair Defenses: Disable or Modify Tools
TECHNIQUE_ID
T1562.001
DESCRIPTION
Batloader executes open-sourced scripts that attempt to stop services related to security software, such as Windows Defender.
ACTION
System Owner/User Discovery
TECHNIQUE_ID
T1033
DESCRIPTION
Batloader fingerprints the host to determine if it is a legitimate victim. It also checks for user and computer name.


ACTION
Domain Trust Discovery
TECHNIQUE_ID
T1482
DESCRIPTION
Batloader checks if the host is domain joined.
ACTION
Ingress Tool Transfer
TECHNIQUE_ID
T1105
DESCRIPTION
Batloader installs second-stage malware for follow-on actions. If the user is domain-joined, it is known to drop Cobalt Strike, although other malware families have also been observed.
MALWARE
Cobalt Strike Beacon
DESCRIPTION
Backdoor
TOOL
MsiExec.exe
DESCRIPTION
Is abused to run MSI files with malicious custom action scripts
TOOL
Gpg4win
DESCRIPTION
Is abused to decrypt next-stage payloads downloaded by Batloader.
TOOL
NirCmd
DESCRIPTION
Is a command-line utility tool
TOOL
Nsudo
DESCRIPTION
Is abused to run processes with elevated privileges
ACTION
Ingress Tool Transfer
TECHNIQUE_ID
T1105
DESCRIPTION
Batloader later installs legitimate system management and file execution tools to aid in privilege escalation and defense evasion.
ACTION
System Binary Proxy Execution
TECHNIQUE_ID
T1218
DESCRIPTION
Batloader bypasses process and/or signature-based defenses by abusing legitimate tools.
TOOL
Syncro
DESCRIPTION
Batloader abuses legitimate remote admin tools, such as Syncro, to facilitate ransomware deployment. Syncro is more likely to be deployed in an enterprise environment.
TOOL
PowerShell
DESCRIPTION
Is abused to run malicious PowerShell scripts
TOOL
Mshta.exe
DESCRIPTION
Is abused to execute malicious code appended to PE files


ACTION
Taint Shared Content
TECHNIQUE_ID
T1080
DESCRIPTION
Batloader abuses legitimate file sharing services to host malware payloads.
ACTION
Credential Access
TACTIC_ID
TA0006
DESCRIPTION
The second-stage malware, such as Cobalt Strike, reaches out to its own C2 server for follow-on actions, such as credential theft.
MALWARE
Cobalt Strike Beacon
DESCRIPTION
Backdoor
ACTION
Data Encrypted for Impact
TECHNIQUE_ID
T1486
DESCRIPTION
Water Minyades generally attempts to facilitate ransomware using Syncro.
TOOL
Syncro
DESCRIPTION
Batloader abuses legitimate remote admin tools, such as Syncro, to facilitate ransomware deployment. Syncro is more likely to be deployed in an enterprise environment.