BianLian Ransomware Expanding C2 Infrastructure and Operational Tempo

rhisac.org/threat-intelligence/bianlian-ransomware-expanding-c2-infrastructure-and-operational-tempo/

September 2, 2022

The threat actors behind the BianLian Ransomware are rapidly expanding infrastructure, and it has been observed targeting manufacturing organizations.

Context

On September 1, 2022, researchers at the cybersecurity firm Redacted published a technical analysis of the BianLian ransomware. In the past month, BianLian has been observed being deployed against numerous sectors, including manufacturing, healthcare, and education. Throughout August, Redacted researchers reported observing BianLian threat actors rapidly expanding their command and control (C2) infrastructure and increasing their attack rate.

Technical Analysis

BianLian is written in the Go programming language, likely to frustrate reverse engineering efforts by security researchers and to make compromising multiple platforms easier for the threat actors deploying the ransomware.

According to Redacted researchers, the threat actor appears technically sophisticated in compromising targeted networks, but is likely inexperienced at ransomware operations, based on the following behaviors observed during the investigation:

- Mistakenly sending data from one victim to another.
- Possessing a relatively stable backdoor toolkit but have an actively developing encryption tool with an evolving ransom note.
- Long delays in communications with victims.
- Through the group's own admission on their onion site, the business side of their infrastructure is unreliable.

Redacted researchers also noted that the BianLian threat actors targeted the ProxyShell vulnerability chain (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) and SonicWall VPN devices to gain initial access into victim networks. The threat actors also employ Living off the Land (LOL) methodology to move laterally, adjusting operations based on defensive controls present on infected networks.

Mitigation Options

Researchers with Redacted provided the following defensive measures:

- An aggressive, prioritized patching regime.
- Employ multi-factor authentication on every system that allows that as an option.
- Visibility into your network and endpoint devices to quickly identify breaches.
- Secure backups to allow return to business operations as soon as possible.
- A well-practiced incident response plan, so everyone involved knows their role.
- An assessment of your "Crown Jewels" that can be used to both inform your security posture and decide ahead of an incident what data you could afford to have leaked so you can avoid paying the ransom.

In addition to these strategic recommendations, there are multiple opportunities for behavioral detections in the attack chain leveraged by BianLian:

- Defense Evasion: Svchost not a child of services.exe
  BianLian called one of their LOL tools svchost, then launched it via a process other than services.exe.
- Defense Evasion: Svchost executing from an unusual path
  BianLian called one of their LOL tools svchost.exe, then executed it from a non-standard path.
- Defense Evasion: Netsh to modify firewall rules
  BianLian leveraged netsh to add a firewall rule to open 3389 to Remote Desktop.
- Reconnaissance: Ping -4 -n 1
  BianLian used single pings to perform network reconnaissance. This is a false-positive prone alert.
- Lateral Movement: Winrm dropping a file via PowerShell
  The binary wsmprovhost.exe is used to mediate the relationship between WinRM and PowerShell. Alerting on file modification by wsmprovhost.exe proved a reliable method to detect BianLian dropping malicious files.
- Lateral Movement: Unknown Binary Established Connection on 3389
  If leveraging an EDR that classifies binaries as known and unknown and ties network connections to binaries, looking for 3389 in use by unknown binaries can be extremely fruitful. This rule detects BianLian's custom Go backdoor.
- Credential Access: Account manipulation via net.exe
  "Net user" is too loud to alert on in most environments, but we recommend alerting on a threshold of "net user" executions. Even a threshold as high as 10 events in 15 minutes would have detected BianLian in the attacks witnessed.
- Execution: Unknown binary launching PowerShell
  If leveraging an EDR that classifies binaries as known and unknown, searching for unknown binaries launching PowerShell will frequently detect use of the BianLian backdoor
- Defense Evasion: Reg.exe modifying safeboot keys
  BianLian added a remote access tool to safeboot keys in order to enable network access for their remote access tool in safeboot.

IOCs

Redacted researchers provided the following indicators of compromise:

Indicator	Type	Notes
104.207.155[.]133	IP Address	Historical IP
104.238.61[.]153	IP Address	Historical IP
146.70.44[.]248	IP Address	Historical IP
155.94.160[.]241	IP Address	Historical IP

167.88.15[.]98	IP Address	Historical IP
172.96.137[.]107	IP Address	Historical IP
188.166.81[.]141	IP Address	Historical IP
194.26.29[.]131	IP Address	Historical IP
194.5.212[.]205	IP Address	Historical IP
194.58.119.159	IP Address	Historical IP
198.252.108[.]34	IP Address	Historical IP
202.66.72[.]7	IP Address	Historical IP
208.123.119[.]145	IP Address	Historical IP
209.141.54[.]205	IP Address	Historical IP
23.227.198[.]243	IP Address	Historical IP
23.94.56[.]154	IP Address	Historical IP
43.155.116[.]250	IP Address	Historical IP
45.144.30[.]139	IP Address	Historical IP
45.92.156[.]105	IP Address	Historical IP
5.188.6[.]118	IP Address	Historical IP
5.230.67[.]2	IP Address	Historical IP
85.13.116[.]194	IP Address	Historical IP
85.13.117[.]219	IP Address	Historical IP

89.22.224[.]3	IP Address	Historical IP
104.225.129[.]86	IP Address	Active IP
104.238.223[.]10	IP Address	Active IP
104.238.223[.]3	IP Address	Active IP
109.248.6[.]207	IP Address	Active IP
13.49.57[.]110	IP Address	Active IP
144.208.127[.]119	IP Address	Active IP
146.0.79[.]9	IP Address	Active IP
157.245.80[.]66	IP Address	Active IP
16.162.137[.]220	IP Address	Active IP
165.22.87[.]199	IP Address	Active IP
172.93.96[.]61	IP Address	Active IP
172.93.96[.]62	IP Address	Active IP
18.130.242[.]71	IP Address	Active IP
185.108.129[.]242	IP Address	Active IP
185.225.69[.]173	IP Address	Active IP
185.56.80[.]28	IP Address	Active IP
185.62.58[.]151	IP Address	Active IP
185.69.53[.]38	IP Address	Active IP

192.145.38[.]242	IP Address	Active IP
192.161.48[.]43	IP Address	Active IP
192.169.6[.]232	IP Address	Active IP
37.235.54[.]81	IP Address	Active IP
45.9.150[.]132	IP Address	Active IP
5.2.79[.]138	IP Address	Active IP
51.68.190[.]20	IP Address	Active IP
54.173.59[.]51	IP Address	Active IP
62.84.112[.]68	IP Address	Active IP
64.52.80[.]120	IP Address	Active IP
66.135.0[.]42	IP Address	Active IP
83.136.180[.]12	IP Address	Active IP
85.13.117[.]213	IP Address	Active IP
85.13.117[.]218	IP Address	Active IP
91.199.209[.]20	IP Address	Active IP
95.179.137[.]20	IP Address	Active IP
1fd07b8d1728e416f897bef4f1471126f9b18ef108eb952f4b75050da22e8e43	SHA256	Encryptor
b60be0b5c6e553e483a9ef9040a9314dd54335de7050fed691a07f299ccb8bc6	SHA256	Encryptor
cbab4614a2cdd65eb619a4dd0b5e726f0a94483212945f110694098194f77095	SHA256	Encryptor
eaf5e26c5e73f3db82cd07ea45e4d244ccb3ec3397ab5263a1a74add7bbcb6e2	SHA256	Encryptor

001f33dd5ec923afa836bb9e8049958decc152eeb6f6012b1cb635cff03be2a2	SHA256	Backdoor
1a1177363be7319e7fb50ac84f69acb633fd51c58f7d2d73a1d5efb5c376f256	SHA256	Backdoor
20bab94e6d9c8ed4832ce3b58f9150b16f9e5f40ffdcb747e10366cab5a30352	SHA256	Backdoor
36281d02e28dd26a1db37ebe36941fc9eb1748868e96b544f227b3b59de51fea	SHA256	Backdoor
3bdcc81931687abac9e6ba4c80d4d596cebb470c80f56213aa29d3da43925537	SHA256	Backdoor
50c86fb27bed1962903a5f9d155544e3fdb859ae19e967a10f0bf3a60bb8954f	SHA256	Backdoor
5d429e05cede806ecea2e99116cac09558fcc0011095201e66c2e65c42f80fcf	SHA256	Backdoor
64065c29b369881ee36314c0d15e442510027186fd9087aec0f63e22a5c6f24c	SHA256	Backdoor
6d7009df2fa033f7adc30793ebd5254ef47a803950e31f5c52fa3ead1197599f	SHA256	Backdoor
8084eddfdb157edf8b1c0cdf8bf4d4e4aaa332fc871c2892aa4113b5148ac63e	SHA256	Backdoor
8592862cd28bcc23cfbcf57c82569c0b74a70cd7ea70dbdee7421f3fafc7ecaf	SHA256	Backdoor
86a9b84c6258c99b3c3c5b94a2087bc76a533f6043829ded5d8559e88b97fb2f	SHA256	Backdoor
9b7a0117a27dc418fbf851afcd96c25c7ad995d7be7f3d8d888fa26a6e530221	SHA256	Backdoor
bb2e9fd9d60f49f0fc2c46f8254e5617d4ec856f40256554087cda727a5f6019	SHA256	Backdoor
c0fe7bfb0d1ffeb61fb9cafeeab79ffd1660ff3637798e315ff15d802a3c974e	SHA256	Backdoor
c7fe3fc6ffdfc31bc360afe7d5d6887c622e75cc91bc97523c8115b0e0158ad6	SHA256	Backdoor
cd17afd9115b2d83e948a1bcabf508f42d0fe7edb56cc62f5cc467c938e45033	SHA256	Backdoor
d602562ba7273695df9248a8590b510ccd49fefb97f5c75d485895abba13418d	SHA256	Backdoor
da7a959ae7ea237bb6cd913119a35baa43a68e375f892857f6d77eaa62aabbaf	SHA256	Backdoor
dda89e9e6c70ff814c65e1748a27b42517690acb12c65c3bbd60ae3ab41e7aca	SHA256	Backdoor
de31a4125eb74d0b7cbf2451b40fdb2d66d279a8b8fd42191660b196a9ac468f	SHA256	Backdoor
f7a3a8734c004682201b8873691d684985329be3fcdba965f268103a086ebaad	SHA256	Backdoor

MITRE TTPs

Redacted researchers provided the following MITRE ATT&CK tactics, techniques, and procedures:

ID	Technique
T1190	Initial Access: Exploit Public-Facing Application
T1047	Execution: Windows Management Instrumentation
T1059.001	Execution: Command and Scripting Interpreter: PowerShell

T1098	Persistence: Account Manipulation
T1078	Persistence: Valid Accounts
T1562.001	Defense Evasion: Impair Defenses: Disable or Modify Tools
T1526.004	Defense Evasion: Impair Defenses: Disable or Modify System Firewall
T1036	Defense Evasion: Masquerading
T1112	Defense Evasion: Modify Registry
T1069	Discovery: Permission Groups Discovery
T1018	Discovery: Remote System Discovery
T1021.001	Lateral Movement: Remote Services: Remote Desktop Protocol
T1021.005	Lateral Movement: Remote Services: VNC
T1021.006	Lateral Movement: Remote Services: Windows Remote Management
T1090	Command and Control: Proxy
T1071.001	Command and Control: Application Layer Protocol: Web Protocol
T1486	Impact: Data Encrypted for Impact