Using Hindsight to Close a Cuba Cold Case

By GuidePoint Security

Published: 2022-02-08 · Archived: 2026-04-06 00:30:18 UTC

Published Feb 8, 2022

Introduction

In September 2021, we released a blog outlining a “Ransomware Near Miss” that began with the exploitation of ProxyShell before deploying Cobalt Strike and a unique RAT for post-exploitation efforts. Luckily, we were able to prevent ransomware from being deployed within the environment during that incident. Fast forward to February 2022, the GuidePoint Security DFIR team found ourselves in familiar territory, but this time Cuba ransomware was deployed throughout the environment, resulting in devastating damage to an organization’s IT systems.

At the time we published the “Ransomware Near Miss” blog, we did not have concrete evidence to firmly link the attack to a specific ransomware family or group. In fact, based on the tools deployed during that incident, we suspected possible links to the Conti group. However, as more intelligence has developed, we believe there are strong indications that the “Ransomware Near Miss” can be attributed to the Cuba Ransomware Group.

Let’s take a look.

A Recent Cuba Attack and the Links to the “Ransomware Near Miss”

In early February, GuidePoint’s DFIR team was engaged by a client to respond to a confirmed Cuba ransomware attack. The initial intrusion pointed to a misconfiguration on a public-facing server that allowed for the attackers to infiltrate the environment, move laterally, and deploy the ransomware throughout the environment. The .cuba file extension and references within the ransom note were explicit indications of which group we were dealing with.

The first interesting discovery was the use of `DefenderControl.exe` – a utility created by Sordum – that permanently disables Windows Defender on Windows systems. This was the first time the DFIR team had seen the use of this GUI-based defense evasion utility being used by a ransomware threat actor, as opposed to PowerShell scripts or other defense evasion utilities.

Also early in the investigation, a malicious batch script, `shar.bat`, was discovered on multiple systems in the environment. Upon further review, this batch script served a single purpose: to grant full permissions to a series of attached drives (both local and remote) for the `Everyone` group and then delete itself from the system.

```
@ echo off
net share C=C:\ /grant:everyone,FULL
net share D=D:\ /grant:everyone,FULL
net share E=E:\ /grant:everyone,FULL
net share F=F:\ /grant:everyone,FULL
<...snip...>
net share Q=Q:\ /grant:everyone,FULL
net share R=R:\ /grant:everyone,FULL
net share S=S:\ /grant:everyone,FULL
net share T=T:\ /grant:everyone,FULL
del "%~f0"
```

Figure 1: Contents of shar.bat

As the ransomware investigation continued, GuidePoint intelligence analysts began researching and correlating additional indicators of compromise (IOCs) associated with Cuba ransomware and the group's tactics, techniques, and procedures (TTPs). As we analyzed our internal and external data sets, pivoting on `shar.bat`, we found two pieces of open-source intelligence (OSINT) that pointed to some familiar IOCs. This is where things began to get interesting, and we started flashing back to the "Ransomware Near Miss."

The first OSINT source we found was a VirusTotal Collection for Cuba Ransomware that we discovered while reviewing `shar.bat`'s VirusTotal entry. One additional IOC within the collection immediately stood out as interesting, `Agent32.bin`, and was especially interesting because it was one of the novel tools we saw used in the September 2021 "Ransomware Near Miss." Pivoting on Cuba intelligence further, we found the November 2021 FBI Flash Alert for Cuba Ransomware. The IOCs section from this report also named `komar.ps1` and `Agent32.bin`, as well as their corresponding SHA256 hashes, as known indicators for the Cuba group. `Komar.ps1` is the malicious PowerShell downloader associated with `Agent32.bin` and was also observed in the "Near Miss."

At this point, we retroactively assessed with high confidence that attribution for the "Ransomware Near Miss" belonged to the Cuba Ransomware Group (UNC2596).

So What About Those Links to Conti Tools?

During the "Ransomware Near Miss" blog we originally made some connections to some of the defense evasion and exfiltration tools used in the incident that were observed as part of the Conti Affiliate Leak. During analysis, we were hesitant to attribute the attack to the Conti group based only on the observation of tools that were now publicly available due to the leak. Hindsight being what it is, we now see the double-edged sword of threat actor tool leaks. The original leak was reported early in August 2021, and by September 2021 these tools were being

used by the Cuba group to perform defense evasion and data exfiltration as a precursor to ransomware deployment. To the Cuba group's benefit, we were unable to attribute the attack to them during the initial investigation due to obfuscation by tools reuse.

Recommendations

The cyber threat landscape continues to feature common themes that we have observed for years. Misconfigurations and lack of alerting capabilities are still one of the most prevalent gaps in cyber defense programs across all industries. Consider pursuing these recommendations to help reduce the likelihood of a ransomware attack in your environment:

- **Monitor your attack surface**, including public-facing infrastructure, for misconfigurations or undesirable configurations that may lead to unauthorized access into the environment.
    - Consider multi-factor authentication and additional logging to identify anomalous access on these systems.
- **Ensure that EDR and other behavioral detection mechanisms are enabled** and being actively reviewed in the environment.
- **Actively pursue threat intelligence capabilities and integrations** within your cyber defense function.
    - Maturing threat intelligence capabilities helps blue teamers stay up to date with threat actor IOCs and TTPs
- **Ensure that you are administratively prepared for a ransomware event** by pursuing tabletop exercises and developing playbooks for effective response.

Conclusion

Over the past few years, ransomware groups have proven how quickly and effectively they can pivot and change tactics at will. There is no exception for the Cuba ransomware group. They have demonstrated a willingness to utilize third-party tools, regardless of their origin, as a strategy for the lowest effort and highest return. This strategy has afforded them the opportunity to fly under the radar in some circumstances where custom tooling might have outed them more quickly.

Ransomware groups continue to undoubtedly be one of the biggest threats in the cyber world; however, as this blog shows, we continue to pursue connecting the dots, sometimes retroactively, and develop threat intelligence to discover, attribute, slow, and hopefully stop more ransomware attacks. Our goal is to use threat intelligence to accomplish these goals and give the blue team the ability to make threat actors' lives harder for a change.

Indicators of Compromise

Indicator	Type	Description
c:\windows\temp\komar.ps1	Filename	Malicious PowerShell Script – Downloader for Agent32.bin
shar.bat	Filename	Batch script to alter drive permissions

C:\Windows\Temp\run.txt	Filename	Malicious PowerShell Script – Downloader for Komar.ps1
45[.]32[.]229[.]66	IPv4 Address	Server Hosting Payloads
108[.]62[.]12[.]122	IPv4 Address	Server Hosting Payloads
4DD315284258A738E7 47250CBA91CB3F	MD5	Agent32.bin
4bbb69bb35f95223e82 a573ce0794a78	MD5	Komar.ps1 (Agent32.bin Downloader)
72a60d799ae9e4f0a34 43a2f96fb4896	MD5	Agent32.bin
4c32ef0836a0af7025e 97c6253054bca	MD5	shar.bat
ba83831700a73661f99 d38d7505b5646	MD5	Komar.ps1 (Agent32.bin Downloader)
ee2f71faced3f5b5b202 c7576f0f52b9	MD5	run.txt
C524CA6A8A86C36A34 FB4DC06A4A2696E80A 1C07	SHA1	Agent32.bin
704d981f358ba00f8297 bdd249f388ed157a0dd1	SHA1	Komar.ps1 (Agent32.bin Downloader)
a304497ff076348e0983 10f530779002a326c264	SHA1	Agent32.bin
86ed4544eeca78dc6488 1a916fe1e1f73dc17f7b	SHA1	shar.bat
209ffbc8ba1e93167bca9 b67e0ad3561c065595d	SHA1	Komar.ps1 (Agent32.bin Downloader)
d1ff26ea3d2d2ced4b7e7 6d971a60533817048d7	SHA1	run.txt
196CD59446AD6BD6258 EDAF94D4845E1A73455	SHA256	Agent32.bin

F87BCAEFF4241606366 B6F7D87		
947c192f7dd6e8329d66f aaa8abcb6b5f59fc7fd8ad af19811da4a4e8b463983	SHA256	Komar.ps1 (Agent32.bin Downloader)
6d5ca42906c60caa7d3e0 564b011d20b87b175cbd 9d44a96673b46a82b07d f68	SHA256	Agent32.bin
1d142c36c6cdd393fe543 a6b7782f25a9cbafca17a 1cfa0f3fc0f5a9431dbf3f	SHA256	shar.bat
79d6b1b6b1ecb446b0f49 772bf4da63fcec6f6bfc7c2 e1f4924 cb7acbb3b4f53	SHA256	Komar.ps1 (Agent32.bin Downloader)
5cd95b34782ca5acf8a34 d9dc184cb880a19b6edca f4a4553fa0619b597c2f50	SHA256	run.txt
hxxp://45.32.229.66/komar.ps1	URL	Malicious PowerShell Script – Downloader for Agent32.bin
hxxp://108[.]62[.]12[.]122/Agent32.bin	URL	Download URL for Agent32.bin

Related Articles
