Focus on DroxiDat/SystemBC

securelist.com/focus-on-droxidat-systembc/110302/

Authors

 Kurt Baumgartner

Unknown Actor Targets Power Generator with DroxiDat and Cobalt Strike

Recently we pushed a report to our customers about an interesting and common component of the cybercrime malware set – SystemBC. And, in much the same vein as the 2021 Darkside Colonial Pipeline incident, we found a new SystemBC variant deployed to a critical infrastructure target. This time, the proxy-capable backdoor was deployed alongside Cobalt Strike beacons in a south African nation's critical infrastructure.

Kim Zetter closely reviewed the preceding Colonial Pipeline incident in her BlackHat 2022 keynote "Pre-Stuxnet, Post-Stuxnet: Everything Has Changed, Nothing Has Changed", calling it a "watershed moment". We are now seeing targeting and tactical similarities elsewhere in the world.

A lot of abstract content and interesting trend analysis has been published about industrial ransomware attacks "The second quarter of 2023 proved to be an exceptionally active period for ransomware groups, posing significant threats to industrial organizations and infrastructure", but very little technical detail in the way of particular electric utility ransomware incidents has been publicly reported. We know that surveyed utilities, on a

global basis, are reporting more and more in the way of targeted activity and higher risk: “56% [of respondents] report at least one attack involving a loss of private information or an outage in the OT environment in the past 12 months”. While not all of the activity is attributed to ransomware actors, perhaps the relevant ransomware attackers are avoiding retaliation by strong government agencies and alliances, while continuing to act on a game plan that demonstrated previous successes. Regardless, this increased utilities targeting is a real world problem with serious potential consequences, especially in areas where network outages may affect customers on a country-wide basis.

Notably, an unknown actor targeted an electric utility in southern Africa with Cobalt Strike beacons and DroxiDat, a new variant of the SystemBC payload. We speculate that this incident was in the initial stages of a ransomware attack. This attack occurred in the third and fourth week of March 2023, as a part of a small wave of attacks involving both DroxiDat and CobaltStrike beacons across the world. DroxiDat, a lean ~8kb variant of SystemBC serving as a system profiler and simple SOCKS5-capable bot, was detected in the electric utility. The C2 infrastructure for this electric utility incident involved an energy-related domain “powersupportplan[.]com” that resolved to an already suspicious IP host. This host was previously used several years prior as a part of an APT activity, raising the potential for an APT-related targeted attack. While our interest was piqued, a link to that previous APT was never established, and was likely unrelated. Ransomware was not delivered to the organization, and we do not have enough information to precisely attribute this activity. However, in a healthcare related incident involving DroxiDat around the same timeframe, Nokoyawa ransomware was delivered, along with several other incidents involving CobaltStrike sharing the same license_id and staging directories, and/or C2.

DroxiDat/SystemBC Technical Details

The DroxiDat/SystemBC payload component is interesting in its own right as a changing, malicious backdoor, often used as a part of ransomware incidents. Multiple “types” of SystemBC have been publicly catalogued. The SystemBC platform has been offered for sale on various underground forums at least since 2018 as a “malware as a service,” or MaaS. This platform is made up of three separate parts: on the server side, a C2 web server with admin panel and a C2 proxy listener; on the target side is a backdoor payload. Regarding an earlier SystemBC variant, other researchers have stated that “SystemBC is an attractive tool in these types of operations because it allows for multiple targets to be worked at the same time with automated tasks, allowing for hands-off deployment of ransomware using Windows built-in tools if the attackers gain the proper credentials.”

This DroxiDat variant is very compact compared to previous and common 15-30kb+ SystemBC variants. Detected SystemBC objects going back to at least 2018 (a SystemBC executable compiled in July 2017 was observed) have numbered in the thousands and were used by a long list of ransomware affiliates. In fact, it appears that most of the functionality

provided in previous SystemBC payloads was stripped from its codebase, and the purpose of this DroxiDat malware variant is a simple system profiler – its file name suggests its use case as “syscheck.exe”. It provides no download-and-execute capabilities, but can connect with remote listeners and pass data back and forth, and modify the system registry. Also interesting, within this power generator network, DroxiDat/systemBC was detected exclusively on system assets similar to past DarkSide targets. And, a Darkside affiliate hit Electrobras and Copel energy companies in Brazil in 2021. The combination of C:\perflogs for storage with DroxiDat/SystemBC and CobaltStrike executable objects was used in past Egregor and Ryuk incidents as well.

MD5	8d582a14279920af10d37eae3ff2b705
SHA1	f98b32755cbfa063a868c64bd761486f7d5240cc
SHA256	a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e
Link time	Thu, 15 Dec 2022 06:34:16 UTC
File type	PE32 executable (GUI) Intel 80386, for MS Windows
File size	8192 bytes
File path	C:**perflogs\syscheck.exe**

Two instances of this DroxiDat malware appeared in C:**perflogs** alongside two Cobalt Strike beacons on multiple systems.
Essentially, this variant provides several functions:

- Retrieves active machine name/username, local IP and volume serial information.
- Instead of creating an exclusive-use mutex, it checks and then creates a new thread and registers a window, class “Microsoft” and text “win32app” (included in all variants of systemBC).
- Simple xor decrypts its C2 (IP:port) settings and creates a session to the remote host.
- Encrypts and sends collected system information to the C2.
- May create and delete registry keys and values.

Missing from this Windows variant that is common to past variants:

- File creation capability.
- File-execution switch statement, parsing for hardcoded file extensions (vbs, cmd, bat, exe, ps1) and code execution functionality.
- Mini-TOR client capabilities.
- Emisoft anti-malware scan.

The object contains xor-encoded configuration settings:

```
XOR KEY:
0xB6108A9DB511264DB3FAFDB74F3D7F22ECCFC2683755966371A3974A1EA15A074404D96B6510
CEE6
HOST1: 93.115.25.41
HOST2: 192.168.1.28
PORT1: 443
```

So in this case, its immediate C2 destination is 93.115.25.41:443
Up until November 2022, this IP host provided bitcoin services. Ownership likely changed in December 2022, as the above backdoor was compiled mid-December.
A second DroxiDat executable was sent down to the same systems with capabilities to add executable entries to the “Software\Microsoft\Windows\CurrentVersion\Run” registry key with a “socks5” entry, i.e.:

```
1  powershell.exe -windowstyle hidden -Command "c:\perflogs\hos.exe"
```

A third DroxiDat object, this time a dll, was sent down to a server.

MD5	1957deed26c7f157cedcbdae3c565cff
SHA1	be9e23e56c4a25a8ea453c093714eed5e36c66d0
SHA256	926fcb9483faa39dd93c8442e43af9285844a1fbbe493f3e4731bbbaecffb732
Link time	Thu, 15 Dec 2022 06:07:31 UTC
File type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
File size	7168 bytes
File path	c:**perflogs**\svch.dll

It implements essentially the same functionality as “syscheck.exe” above without the ability to modify the registry. It also maintains the same HOST and PORT values, and 40-byte key.

Cobalt Strike beacons and related infrastructure

Cobalt Strike beacons were detected on these systems as well, located in the same directory and similar infrastructure. In a couple of instances, the beacons arrived and were detected on the same day as DroxiDat. In several instances, a couple of the beacons first arrived and were detected in the same perflogs directory two days later, and several more six days later. It’s highly likely that the same attackers maintained access via stolen credentials or another unknown method.

The beacons' infrastructure was power-utility themed:
`powersupportplan[.]com, 179.60.146.6`
`URL: /rs.css, /skin`

Several beacons calling back to this C2 included the same license_id value:
`"license_id": "0x282d4156"`

We identified one other Cobalt Strike C2 server and beacon cluster, possibly spoofing a power-utility theme as well, along with other related data points: `epowersoftware[.]com, 194.165.16.63.`

The ssh server on this epowersoftware host shares the same ssh version and RSA key(s) with the one at powersupportplan[.]com. Additionally, the CS beacon calling back to this domain maintains the same license_id, as seen above: "license_id": "0x282d4156".

Attribution

We have a consistent set of data points across multiple incidents mentioned in our private report, helping suggest an assessment may be made with low confidence. Several of these suggest this activity may be attributed to Russian-speaking RaaS cybercrime. In this case, we may be looking at an activity from a group known as Pistachio Tempest or FIN12, a group HHS reported "has specifically targeted the healthcare industry" in 2022, frequently deploying SystemBC alongside CS Beacon to deploy ransomware:

- Consistent use of the same perflogs staging directory across this intrusion set within an early 2023 timeframe.
- SystemBC consistently paired alongside Cobalt Strike.
- Shared profile data across Cobalt Strike hosts.
- Nokoyawa ransomware deployment alongside DroxiDat within a health care organization early 2023.

More details can be found in our private crimeware intelligence report "Focus on DroxiDat/SystemBC – Unknown Actor Targets Power Generator with DroxiDat and CobaltStrike" released in June 2023.

Reference IoC

Domains and IP

93.115.25.41
powersupportplan[.]com, 179.60.146.6

Likely related
epowersoftware[.]com, 194.165.16.63

File hash

Droxidat
8d582a14279920af10d37eae3ff2b705
f98b32755cbfa063a868c64bd761486f7d5240cc
a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e

CobaltStrike beacon
19567b140ae6f266bac6d1ba70459fbd
fd9016c64aea037465ce045d998c1eead3971d35
a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4

File paths, related objects

C:\perflogs\syscheck.exe
C:\perflogs\a.dll
C:\perflogs\hos.exe
C:\perflogs\host.exe
C:\perflogs\hostt.exe
C:\perflogs\svch.dll
C:\perflogs\svchoct.dll
C:\perflogs\admin\svcpost.dll
C:\perflogs\admin\syscheck.exe
C:\perflogs\sk64.dll
C:\perflogs\clinic.exe

SystemBC is like Christmas in July for SOCKS5 Malware and Exploit Kits
They're back: inside a new Ryuk ransomware attack

- Backdoor
- Malware Descriptions
- Malware-as-a-Service
- Ransomware
- Targeted attacks

Authors

 Kurt Baumgartner

Focus on DroxiDat/SystemBC

Your email address will not be published. Required fields are marked *