

ICS Threats: Malware Targeting OT? It's More Common Than You Think

forescout.com/blog/targeting-ot-security-ics-threats-malware/

October 22, 2024

Malware targeting operational technology (OT) and industrial control systems (ICS) is evolving. While OT-specific malware remains rare, our latest research indicates that generic malware, such as botnets, is increasingly targeting OT devices.

We've analyzed recent submissions on VirusTotal and uncovered various botnet clusters (e.g., Aisuru, Kaiten, Gafgyt) that exploit OT default credentials and wipe data directories. These discoveries highlight the growing risk to OT environments beyond specialized malware from opportunistic attacks by generic threats.

To protect against these risks, organizations must identify and secure exposed OT and ICS devices, update default credentials, and monitor networks for malicious activity.

Motivation: A Brief History of ICS Threats: Malware Targeting OT

Hundreds of thousands of new malware samples are created by threat actors daily — and are often submitted to public repositories like VirusTotal. Most of these target IT systems running Windows on x86 or x64 architectures. Remote access trojans (RATs) and infostealers are the most common malware categories, as reported in our [2023 threat roundup](#).

However, since the infamous Mirai botnet emerged in 2016, [malware targeting Internet of Things \(IoT\) devices](#) has surged in the form of DDoS botnets infecting embedded systems. DDoS botnets were the third most popular malware category in our threat roundup. Additionally, we recently [published research](#) about botnets that go beyond DDoS to wipe IoT devices.

Historically, OT-specific malware was extremely rare. Between 2010 and 2017 only five OT-targeting malware were identified (Stuxnet, Havex, BlackEnergy3 Industroyer and Triton). However, since 2022 there have been five more significant OT malware discoveries, including [Industroyer2](#) and [INCONTROLLER](#) in 2022, [COSMICENERGY](#) in 2023, Fuxnet and [FrostyGoop/BUSTLEBERM](#) in 2024.

Additionally, several other malware, such as VPNFilter with its Modbus protocol module, and Acid Rain, indirectly impacted OT systems — while some ransomware (like EKANS) target OT-related Windows processes.

Several of these malware, including COSMICENERGY, FrostyGoop/BUSTLEBERM and AcidRain, were first found on public repositories. Our recent research took a closer look at VirusTotal around the time of the latest major discovery, FrostyGoop/BUSTLEBERM, to hunt for other OT-related threats. What we found reveals the broader landscape of potential risks to OT systems.

The Hunt: Searching for OT/ICS Malware on VirusTotal

OT-specific malware often interacts with OT devices using engineering protocols like Modbus (FrostyGoop/BUSTLEBERM), IEC-104 (Industroyer), or S7 (Stuxnet). These malware types frequently contain tell-tale strings, such as protocol names or specific credentials, which can serve as 'signatures' to identify OT capabilities. In many cases, these malware directly used or at least based their code on [open source libraries implementing these protocols](#).

We developed a YARA rule with 136 OT-related signatures across several protocols, as below.

Protocol	Languages	#Signatures
Modbus	Go, C/C++	26
Bacnet	Go, C/C++	29
S7	Go, C/C++	6
OPC-UA	Go, C/C++, Python, Rust	47
IEC-104	Go, C/C++	11
EtherNet/IP	Go, C/C++	8
DNP3	C/C++	7
Profinet	C/C++	6

For Go, the signatures are based on the names of open-source libraries. We identified more than 40 of those. For the other languages, the signatures are based on either debug strings or byte sequences on binaries.

Using VirusTotal's RetroHunt service, we analyzed files submitted for a three-month period (between June 11 and September 11, 2024). Our hunt matched 989 files: 55% were Windows executables and 45% were ELF executables for Linux/Unix-like systems. These files were compiled for 15 different CPU architectures. The majority (66%) targeted x86 or x64 architectures and 21% targeted ARM flavors.

The figure below summarizes the file distribution per protocol. The most common protocol was Modbus, which is also the most exposed and the most attacked OT protocol. The sum is larger than the 989 unique samples because some files match more than one protocol.

After analyzing these files, we categorized them as either benign (involving legitimate OT protocol interactions, firmware or network inspection tools) or malicious. Among the malicious ones, we identified three FrostyGoop/BUSTLEBERM samples — which aligns to the timing of that malware's discovery. And, 19 samples were linked to botnet-related activity (usually classified generically as either Mirai or Gafgyt in VirusTotal).

Two files were corrupted, making it impossible to determine if they were malicious. Another file exhibited typical malware behavior by using shared memory to load executables, but without the loaded binary we couldn't confirm its maliciousness.

Go Deeper: Trends, Threats, and Best Practices

Join Elisa Costante, VP of Research alongside Rik Ferguson, VP of Security Intelligence, as they delve into the changing dynamics of exposed ICS

[Watch Webinar](#)

Overall, only a very small portion of the files caught in this hunt were malicious and an even smaller subset was OT-specific (only the three FrostyGoop/BUSTLEBERM samples). While OT-specific malware is increasingly frequent, it's still not a common occurrence. However, the botnet-related files warrant further investigation.

The Catch: Botnets Wipe 'modbus_rtu' and Infect Via PLC Credentials

All 19 samples identified as Mirai or Gafgyt were flagged by our rule because they contained the string '/mnt/modbus_rtu'. During our investigation, we noticed that several of these samples originated from URLs containing the string "hoho4christmastrees". This led us to broaden our search to include that URL, ultimately resulting in the discovery of 29 samples, as detailed below.

Hash	URL	PL cr
2a4d741b53ddd4c67d8aec976230d7baf1823adb72995d0eb13208a714c9ae2b	http://51.83.180[.]147/hoho4christmastrees/aisuru.mips	Ye
1f8f381d3693024c5f07da079a8cc3391c306ce1a343923bfa3d5ffeade05387	http://45.95.168[.]124/hoho4christmastrees/aisuru.m68k	Ye

1f06e909e60809b062aafc95f3a91626023ec3a237e2053f3e9ca3688844e76	http://45.95.168[.]124/hoho4christmastrees/aisuru.arm5	Ye
2c2cf5a202ede6eadc60beb53175691aabc2bec45140561a827e99f33acc4dc3	http://45.95.168[.]124/hoho4christmastrees/aisuru.m68k	Ye
2ae773d4bdba6352cf8aa7614a487f90ac9963c11dfdabe6e0fc234a1e4b388e	http://45.95.168[.]124/hoho4christmastrees/aisuru.x86	Nc
2e3b33cf88b68c31379145c25e2281b0459f2a61ba8f0dccb44343a26b9b03e7	http://45.95.168[.]124/hoho4christmastrees/aisuru.m68k	Nc
2c816f39d4688c0378f407390f5861b87b0abd4ef193818081f8bb0fa70d3b44	http://45.95.168[.]124/hoho4christmastrees/aisuru.mpsl	Ye
008ec11993e76270a1997c90ed6888e311dc786c4ce82e0167ddf6172763bba5	http://45.95.168[.]124/hoho4christmastrees/aisuru.arm7	Ye
02755b1c062b93ef09171c38e55c24563dd966ae76ad4fbb33af410de0d7d7d4	http://45.95.168[.]124/hoho4christmastrees/aisuru.mips	Ye
2a5df90918f490042280402d86ef29e085c12852a9f194cd4467c0b34aa374c7	N/A	Ye
1fca9720f3c92d303a4aadeeda3fca9f42f28e91e7ce88d3ac9dd23423a5d93e	http://45.95.168[.]194/hoho4christmastrees/aisuru.arm	Ye
2b5ed468f201a70dbcaf158ed8cea76b337ef5da620b08640b9986cb193684a0	N/A	Ye
2bb58157fba2b68bdfbee6ce00387a4d2308146ed866dcf90bf184d148e066e	http://45.95.168[.]194/hoho4christmastrees/aisuru.arm6	Ye
1ef0e76b4f9f4b8582d5c5d94ff288b9d139a7214940e230ec3d578ca9802b2a	http://45.95.168[.]194/hoho4christmastrees/aisuru.arm	Ye
02a2896b5be54064c1d7ba39ef208f73a4804d35c56a1a96bf84c46cf4c88534	http://206.126.81[.]82/hoho4christmastrees/aisuru.arm	Ye
014ff5304e126366dd0b523ed0eb11dbb9713156d95b394e0a183022f20dbf	http://206.126.81[.]82/hoho4christmastrees/aisuru.arm5	Ye
00599b5e256bada49a8a85e86f0c50ea6130c262c7fa31eb650e29d3529b93f5	http://206.126.81[.]92/hoho4christmastrees/aisuru.ppc	Ye
2bb2e6113c22fe6f8aa00840c8196369fe10dc19c2212aa109d6ef47a7db4bff	http://206.126.81[.]92/hoho4christmastrees/aisuru.ppc	Ye
2abd99d46cd346fbab3df035f9071d7f468123839670c181bbdd7862f70224ed	http://206.126.81[.]92/hoho4christmastrees/aisuru.m68k	Ye
1f0b69f697162e528e8c0b05f978c584e602ed375cd578df38a83db9c07a0c94	http://206.126.81[.]92/hoho4christmastrees/aisuru.mpsl	Nc
0266bfc667dddf8abde6afa3528b6161017e4350f1cdb78af9567f658d30b7f2	N/A	Ye
1f5805c0db5a793d1e12f8134ebb1c331d6fe3bd9b2d0d2ef1e00bc3da3755da	http://206.126.81[.]105/hoho4christmastrees/aisuru.mpsl	Nc
1f7eccc8544053660a1c330a77162a320edf84aa2ede7214ccc5571c8623bc2d	N/A	Ye
0048005413f12b2abe236c5c7fc1c7a7f086d94fd34ea342e5933eb84ca1e204	N/A	Ye
2f888d6bbf43c29e27da3ef6a3d98db4604e26cd95ad2abc56b0c3bd6a1af09b	N/A	Ye
023b2df45e9a2e370196a520571d2f91c0da5dda66e3378219fd0ca790f513a4	N/A	Ye
2cffd3fb7764d08bbf6b9f504584b96ef2b6e98f782efb53f91a5f5516d4dcb7	N/A	Ye
2eee0015aa2b746eb799d085d43e60e35c7ec0ed260df6de93aa3ef575d3bffd	N/A	Ye
1f3814d7c3774b7d7109e02db426ff74e8f3c51922332fe35badef897dca8c4b	N/A	Ye

The table above is organized by the date and time the samples were first submitted to VirusTotal. All were initially submitted between May and August 2020 primarily from Japan — with the exception of the last seven samples. All samples were re-submitted on July 18, 2024 from India.

The filenames suggest that these samples are a part of the Aisuru botnet which was [first identified around June 2020](#). Interestingly, a botnet with the same name was used in an attack on the [Steam gaming service](#) on August 24, 2024 — though the two incidents seem unrelated.

The table highlights two key details:

Modbus Directory

Samples containing the '/mnt/modbus_rtu' string match the original samples and indicate this botnet's wiping capabilities. This string points to one of the directories that the malware attempts to wipe. While earlier versions of Aisuru did not include this functionality, the wiping capability has been present in every sample since June 10, 2020. For more on IoT wiper behavior, see our [recent blog](#).

PLC Credentials

The malware includes known default credentials for two niche lines of programmable logic controllers (PLCs): [INTEG JNIOR](#) and [Elsist SlimLine](#). These credentials are used to infect the devices and originate from the [original Brickerbot wiper](#) — which did not include the "modbus_rtu" directory. Though these PLCs are relatively uncommon, there are over [700 exposed Elsist](#) devices, mainly located in Italy, as shown below. In addition, the botnet also includes credentials for various IoT devices, such as IP cameras and DVRs.

Expanding the Search: Botnets With Other PLC Credentials

Since we saw botnets using default credentials for niche controllers, we expanded our search to include more widely used default OT/ICS passwords. To do this, we leveraged the Forescout [eyeInspect](#) database which contains hundreds of default credentials for OT devices.

This expanded search uncovered 17 samples from another botnet that used the following known default credentials for various OT products:

Credentials	Product
Liebert:Liebert	Emerson Liebert IntelliSlot Web Card
qbf77101:hexakisoctahedron	Schneider Electric Modicon Quantum
ftpuser:password	Schneider Electric Modicon Quantum
Basisk:Basisk	Siemens Simatic S7-300 (pre-2009 versions)
admin:avocent	Emerson Avocent ACS 6000 Advanced Console Server
sconsole:12345	Sierra Wireless AirLink

These credentials were also mixed with general IoT passwords, but unlike the earlier findings, these samples were more recent. They were all downloaded from a dropper shell script (hash: 86d0b365f87a8fda44d605b072ff08fe349f95c70679461ac48e60933a120490) which was hosted on [http://176.123.1\[.\]32/](http://176.123.1[.]32/) or [http://network\[.\]jirc6\[.\]xyz](http://network[.]jirc6[.]xyz). All the samples were submitted to VirusTotal from the US on August 21, 2024. The identified samples are as follows:

Hash	URL
08d1eaff405a19e32c5afc1aeabba5744a2432c37991fa227b6240e852aee71e	http://176.123.1[.]32/scanirc.i686
e1a7a666ef3ebb1ea910f68b9189367474a20ddba0ee851641691d798f581740	http://176.123.1[.]32/scanirc.x86
ec2c2b4e9c317eb7d7b704d4674619a3abd59823ffe7401b785d7c8d34c1985f	http://176.123.1[.]32/scanirc.i686
4ff458841c8e2c4049064752ad4c3dcfda79fd0b97af7eac7df3b6c53dfa3ef4	http://176.123.1[.]32/scanirc.sh4
d700e4d9cfd2b57057aa2aa30483d0775755ca0c5820098e9e0109b07ded4ba	http://176.123.1[.]32/scanirc.arm6

6004501df7c5a56461c4ce331c900a3f42c017b7166a2703e18ec16003127141	http://176.123.1[.]32/scanirc.sh4
ea57c28ae66512c3334fac383bee67ee03fa24890d3b32fb2d19ff3613d60cd7	http://176.123.1[.]32/scanirc.arm5
20e49b6bd54e0dd6d15c58592857c66be6698287a0bbac1433d0bcf53be161c2	http://176.123.1[.]32/scanirc.mpsl
a21943769803fc4183065470a81384c447941e1d0dedbc4047ed14e8cb204701	http://176.123.1[.]32/scanirc.arm
31136d01edf0305000b87040219cfd36bebd3b5686a07ded8ec5d6fdc77c243c	http://176.123.1[.]32/scanirc.arm7
86fc830c9a5ca82dc314d9718feb517251cb08e9c9e960974784a1ecdb584d2b	http://176.123.1[.]32/scanirc.mips
d475334508362aa070e1a7fdb941df5690b1851d2d6c6e47a40ffeb5c5aa228	http://176.123.1[.]32/scanirc.x86
d78efec23bce6838e73e4910fda7f2823d922744943db40fc77974f1223b99ec	http://176.123.1[.]32/scanirc.mips
127694c50f2217deed62f88adf200bf8dc3469b8cee1da194b598682fc73324a	http://176.123.1[.]32/scanirc.sh4
705fe98e63eaa9401864b57b030ef298cb3bf40750c101f680caefa0b860a558	http://176.123.1[.]32/scanirc.arm7
9358fef1afd21a96551a34048bba92429939712ec95efc58ad6a0d48f947b635	http://176.123.1[.]32/scanirc.ppc
a6ffdcc03878153ef0af086d579bc16dec9083f14c4bfa39704264ef37567fab	http://176.123.1[.]32/scanirc.m68k

The filename ‘scanirc.’ is not linked to any specific botnet family, but these samples include the string “Modified Kaiten” which indicates they are a variant of the Kaiten botnet. This botnet first appeared back in 2016 shortly after the Mirai botnet.

Additionally, 21 other samples of the same “Modified Kaiten” botnet were submitted on July 4, 2024 from the US. These samples were distributed from a different IP address (79.33.237[.]158) and followed a different file naming pattern http://79.33.237[.]158/mq* where ‘*’ represents the target architecture.

We also identified two other clusters using only the “hexakisoctahedron” default password of Schneider Electric Modicon Quantum PLCs:

- One cluster included 32 Gafgyt variant samples, first seen between July 1 and July 24, originating from IP addresses 45.95.146[.]42, 95.214.27[.]246, 91.92.241[.]244 and 154.216.17[.]106.
- Another cluster contained over 150 samples of a distinct Gafgyt variant first seen between July 6 through the end of the analysis period. These samples were downloaded from IP addresses 85.239.34[.]237, 95.214.27[.]246, 185.244.36[.]159, 94.156.71[.]248, 179.43.139[.]194, 193.233.161[.]226, 147.78.103[.]71, 154.216.19[.]71, 185.216.70[.]121, 185.216.70[.]9, 77.90.37[.]71, 94.156.79[.]191.

The targeting of Modicon PLCs is important for several reasons. Modicon PLCs use the Modbus protocol and are widely deployed. This is a line of devices in which we found vulnerabilities in the past. **They are often exposed on the Internet including in critical infrastructure, including hydroelectric power stations and solar farms.** These PLCs have previously been targeted by the OT-specific malware INCONTROLLER, as well as by hackers. Now, botnets, which typically infect exposed IoT devices, are also setting their sights on them.

Currently, over 3,500 Modicon PLCs are exposed online. Not all use the default “hexakisoctahedron” password. This number has been decreasing by 17% over the past few years (from 4,029 devices in June 2021 to 3,339 in June 2024). The most commonly exposed models are the M340 and the M221, as shown below.

Conclusion and Mitigation Recommendations

The key takeaway from this research is that OT-specific malware, while increasing in frequency, is far from the most common threat to OT devices. In fact, exposed OT devices are more frequently targeted by opportunistic attackers, including hackers and generic malware, such as botnets. These attackers exploit well-known credentials and attempt to wipe data, spread malware or launch DDoS attacks.

Through our [Adversary Engagement Environment \(AEE\)](#), we deploy real and simulated purposely-vulnerable OT assets worldwide, such as PLCs, industrial routers and HMIs, to observe threat actor behavior. **The most frequent activity we detect is login attempts using well-known credentials: We've observed over 20,000 attempts between September and October 2024 — for an average of more than 600 per day.**

To safeguard OT environments, we recommend the following measures:

Harden OT Devices

Identify all devices connected to your network, assess their open ports and credentials, and ensure that default or easily guessable credentials are changed. Disable any unused services to minimize attack surface.

Network Segmentation

Avoid directly exposing OT devices to the internet. Follow CISA's guidance on securely providing [remote access for industrial control systems](#). Properly segment networks to isolate IT, IoT and OT devices limiting network connections to only authorized management and engineering workstations or among unmanaged devices that need to communicate.

Monitor for Threats

Implement IoT/OT-aware monitoring solutions that can detect malicious indicators and behaviors. This includes flagging the use of blacklisted credentials and unauthorized OT protocol activity within your network.

Indicators of Compromise (IoCs) including IP addresses and others not listed here for brevity, such as file hashes, are available on the [Forescout Research – Vedere Labs threat feed](#).

Go Deeper: Trends, Threats, and Best Practices

Join Elisa Costante, VP of Research alongside Rik Ferguson, VP of Security Intelligence, as they delve into the changing dynamics of exposed ICS

[Watch Webinar](#)