The Evolution of IoT Linux Malware Based on MITRE ATT&CK TTPs

trendmicro.com/en_us/research/21/l/the-evolution-of-iot-linux-malware-based-on-mitre-att&ck-ttps.html

December 9, 2021

In this blog entry, we share the findings of an investigation on the internet of things (IoT) Linux malware and analyzed how these malware families have been evolving. We relied on the tactics, techniques, and procedures (TTPs) of MITRE ATT&CKto define the malware capabilities and characteristics that we saw.

Our study showed that IoT Linux malware has been steadily evolving, particularly those that are used to create IoT botnets. Capabilities were both added and removed over time. Notably, neither data exfiltration nor lateral movement has been successful for the authors, and they have pivoted instead to centralized infection.

Table 1 shows the 10 most implemented capabilities (or techniques) in our malware data set.

ATT&CK Tactic	Technique (TTP)	Number of malware families
Discovery	File and Directory Discovery (T1083)	10
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	9
Initial Access	External Remote Services (T1133)	8

Execution	Command and Scripting Interpreter: Unix Shell (T1059.004)	7
Impact	Network Denial of Service: Direct Network Flood (T1498.001)	
Credential Access	Brute Force: Password Guessing (T1110.001)	6
Discovery	Process Discovery (T1057)	
Execution	Native API (T1106)	5
Impact	Data Encrypted for Impact (T1486)	
Defense Evasion	Indicator Removal on Host: File Deletion (T1070.004)	4
Lateral Movement	Exploitation of Remote Services (T1210)	
Persistence	Scheduled Task/Job: Cron (T1053.003)	

Table 1. The top 10 most implemented techniques

Methodology

The results presented in this entry are the outcome of a methodology that takes advantage of the power of the MITRE ATT&CK framework to characterize the capabilities of IoT Linux malware. The ATT&CK framework allowed us to describe threats in a structured way and to have an implementation-independent representation that let us compare malware capabilities. The capabilities were extracted by using both static and dynamic analysis, after which we mapped them into the ATT&CK Techniques, Tactics, and Procedures (TTPs).

The methodology is comprised of four steps:

1. Malware collection. We selected malware discovered between January 2019 and August 2021.
2. Malware analysis. We employed both static (Ghidra, IDA Pro) and dynamic analysis (strace, ltrace, GDB) to discover malware capabilities. We looked for all aspects of each malware sample including the pre and post exploitation steps, such as initial access vector, lateral movement, and impact.
3. Mapping. We mapped the malware capabilities to MITRE ATT&CK TTPs.
4. Analysis. We analyzed the mapped TTPs to retrieve changes and similarities in our malware set.

Figure 1 illustrates the steps used in this methodology.

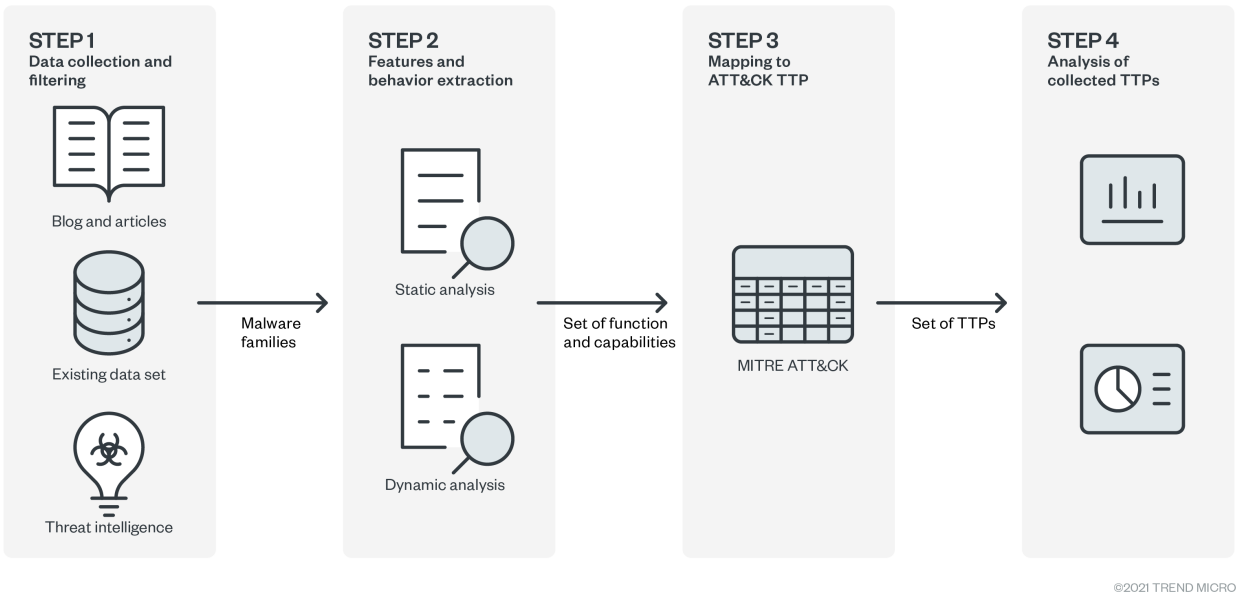

Figure 1. Analysis methodology based on MITRE ATT&CK TTPs.

New IoT botnet techniques

During the observation period, we noted four new techniques added to threat actors' arsenals. One is a newly implemented technique in botnet families called *Masquerading: Match Legitimate Name or Location (T1036.005)*. It is a Defense Evasion technique that likely reflect the manufacturers' increasing interest and efforts in securing these IoT devices or appliances. The technique involves adversaries trying to match the name and location of legitimate and trusted programs to hide malicious executables and evade detection.

Another new technique that diverges from the more common technique being used in IoT Linux malware (Indicator Removal on Host: File Deletion (T1070.004) is *File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification (T1222.002)* introduced in a malware discovered in mid-2020. We observed these additions especially in the Dark Nexus malware. Most of the platforms provide two primary commands used to manipulate file and directory ACLs: chown (change owner) and chmod (change mode).

Furthermore, among the 2021 discovered families, is a variant of StealthWorker GO, a malware written in the Golang language, where we observed the addition of the *Scheduled Task/Job: Cron (T1053.003)* technique. This is an execution tactic which also allows malware to achieve persistence in the system. This software utility maintains persistence in the system by enabling an attacker to achieve time-based command execution.

Dropped techniques

On the other hand, we found three techniques relating to the lateral movement tactic to have been dropped. We observed a trend in recently discovered families that gives the responsibility for propagation back to the C&C server. In the Dark Nexus family, for example,

we found that it is the C&C server that takes steps to propagate the malware. Our analysis highlighted the drop of two techniques linked to the Lateral Movement tactic, which are *Remote Services (T1021)* and *Exploitation of Remote Services (T1210)*. In relation to this, the technique for the discovery of network information, *System Network Configuration Discovery (T1016)*, is also no longer enforced.

Uncommon techniques

Additionally, we noticed that IoT Linux malware authors are not interested in stealing data. In our data set, there is only one malware (QSnatch) that implements typical tactics for data leakages, such as collection and exfiltration. Moreover, we also found that privilege escalation is not among the interests of IoT malware authors. It is likely because, from a malware author's standpoint, the benefits of executing malware that require higher privileges are not worth the effort of implementation. Furthermore, the default accounts on targeted devices usually already come with all the privileges needed to run programs, write to the filesystem, and establish new connections.

Differences between ransomware and botnet malware

The characterization through the ATT&CK matrix also allowed us to compare different malware classes that target IoT devices which in our data set are ransomware and botnet families.

The findings highlight some common techniques, such as the Credential Access methodology where *Brute Force: Password Guessing (T1110.001)* is the most common technique that both malware classes fall under. This finding is not a surprise since it is common to find default usernames and passwords still being used in these kinds of devices. Usually, users are not aware of the risks of exposing IoT devices to the internet. Indeed, many devices are still installed without changing the default credentials or securing remote access.

Another common capability for both classes is *External Remote Services (T1133)* from the Initial Access Tactic, which confirms unsecured and exposed internet services, such as Telnet and SSH. This technique allows attackers to exploit external-facing remote services to initially access and/or persist within a network; they also often use exposed services that do not require authentication.

Another similarity is in the two classes' Command and Control implementation, as both implement *Application Layer Protocol: Web protocol (T1071.001).* This is likely because the market for malware-as-a-service is growing. Thus, having a simple UI that the "customers" or other threat actors can use to control the malware is an important aspect.

By comparing the number of unique TTPs implemented, we studied the implementation variations among different malware families and noticed that while different ransomware families share many common techniques, botnets tend to innovate more and implement a

variety of different TTPs to exploit many services. This may be because detection of botnet malware is more mature, so they require more frequent changes to avoid being easily detected. These differences are illustrated in Figure 2.

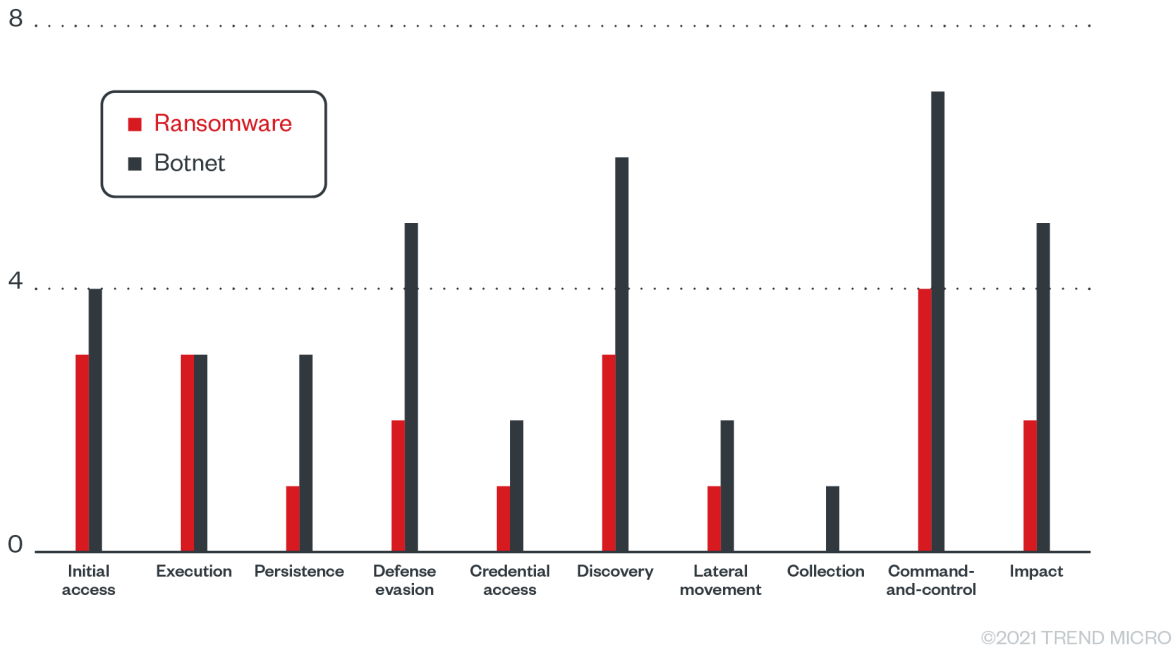

Figure 2. Differences in number of implemented unique TTPs.

Conclusion

As the number of connected devices grow, linked threats also increase. Knowing the evolution of malware that targets IoT devices is fundamental to implementing effective countermeasures and defenses.

We saw how IoT malware has been slowly developing over the years. Botnet threats, in particular, is an active field where capabilities are being added and removed, reflecting not only the behavior of threat actors but also the defenses being implemented in these devices. The MITRE ATT&CK framework helps create a standardized way of listing down techniques and characterizing threats found today. It is easy to see how the awareness of common TTPs can help organizations and users better protect their devices and networks. For example, our findings further stress the importance of changing default passwords in all connected devices.

Organizations and users can also consider these steps to secure their devices:

- Manage vulnerabilities and apply patches as soon as possible. Applying patches as soon as they are released can reduce the chances for potential exploits.
- Use secure configurations. A secure device configuration narrows openings for compromise or remote attacks.

- Use strong, hard-to-guess passwords. Aside from changing default passwords, users can circumvent brute force techniques by using strong passwords and enabling two-factor authentication if it is an option.

IoT

In our study, we relied on the tactics, techniques, and procedures of MITRE ATT&CK to define the malware capabilities and characteristics of IoT Linux malware. We describe our findings and how IoT malware has been evolving.

By: Veronica Chierzi December 09, 2021 Read time: (words)

Content added to Folio