MANDIANT
NOW PART OF Google Cloud

THREAT INTELLIGENCE
WHITE PAPER

Business IoT Targeted by Espionage Groups

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 4.

The number of active Internet of Things (IoT) connected devices is expected to reach nearly 42 billion in 2023[1], helping to accelerate innovation and automation across sectors from smart manufacturing, retail inventory management, digital payments, and physical security and surveillance. As with nearly every technology advancement, cyber risk is a side effect every business must expect.

In the past, Mandiant has observed IoT devices, smart devices, and routers compromised and used to create botnets to perpetrate large scale financially motivated cyber crime operations. A botnet is a network of compromised devices that a threat actor can use to conduct a variety of threat activity, such as distributed-denial-of-service (DDoS) attacks and malware distribution. However, Mandiant assesses with moderate confidence that state-linked espionage groups have also leveraged botnets for multiple purposes[2]. This attacker behavior underscores the opportunity large scale adoption of IoT and smart devices presents for state-linked threat actors looking to acquire strategic intelligence and intellectual property from global businesses.

Organizations looking to continue their digital transformation, accelerate automation, recover lost value chains after the economic impacts of the COVID-19 pandemic, or leverage the rollout of 5G connectivity networks[3] are encouraged to work closely with their cyber security teams to ensure a comprehensive cyber defense plan is in place to help protect the organization.

IoT Device, Smart Device, and Router Botnets Useful for Obfuscating Activity

Mandiant assesses that state-linked espionage groups use botnets consisting of IoT, smart devices, and routers to obfuscate malicious activity, based on multiple campaign observations from Mandiant and other private and public sector security researchers. Reported instances of compromised device botnet use by espionage groups include the following.

- In April 2022 Mandiant reported[4] on a campaign by APT29 using a botnet of IoT cameras as part of command and control (C2) activities using the QUIETEXIT malware (Figure 2). The domains used in this C2 activity appeared designed to blend in with legitimate traffic from the infected IoT devices, apparently to hide the activity from anyone reviewing logs.

1. Frost and Sullivan, Internet of Things (IoT) Predictions Outlook, November 2022
2. Mandiant, Espionage Actors Lurk in Compromised Device Botnets, April 2023
3. Frost and Sullivan, The Top Growth Opportunities for IoT in 2023, March 2023
4. Mandiant, https://www.mandiant.com/resources/blog/unc3524-eye-spy-email

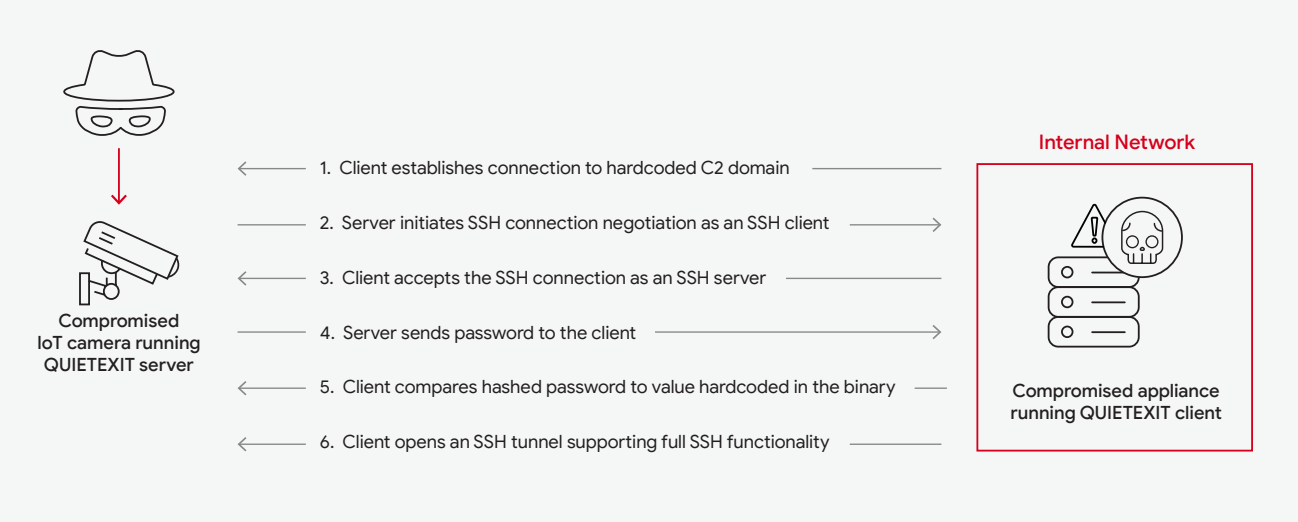

FIGURE 1: How QUIETEXIT works with IoT devices

- A 2021 report[5] from France's Agence nationale de la sécurité des systèmes d'information (ANSSI, French National Agency for the Security of Information Systems) detailed a campaign linked to the Chinese group APT31 that reportedly used a botnet of routers and possibly other small office and home office devices to obfuscate activities within targeted networks.
- In 2022 PricewaterhouseCoopers reported[6] on malware observed during an engagement that they named "BPFDoor," which Mandiant has linked to APT41. In the reported campaign, the malware allegedly received commands from virtual private servers (VPS) that were controlled by a network of Taiwan-based compromised routers.
- Chinese security firm Antiy reported[7] in 2022 that it had observed a large network of compromised IoT devices and Linux devices routing traffic between C2 servers and Torii malware. According to the firm, they were able to attribute the activity to OceanLotus, referred to by Mandiant as APT32; however, Mandiant has not confirmed this attribution.
- In 2018 researchers publicly reported[8] use of VPNFILTER malware in campaigns targeting networking devices and network-attached storage (NAS) devices globally, with a heavy concentration of devices in Ukraine. Some samples reportedly integrated adversary-in-the-middle (aitm) and destructive capabilities, but it is possible[9] that these modules were intended for other purposes. Mandiant believes this use of VPNFILTER is consistent with Russian-sponsored cyber espionage activity.

5. https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-013/
6. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
7. https://mp.weixin.qq.com/s/2RIuW4O56UWiNSQB2hQtGA
8. https://blog.talosintelligence.com/vpnfilter/
9. https://thehackernews.com/2018/06/vpnfilter-router-malware.html

Public reporting and Mandiant observations indicate that some actors have compromised or used existing botnets created by other threat actors. Mandiant suspects that this tactic is useful for espionage actors in very limited circumstances and will therefore not significantly increase in usage in the future.

- In September 2022 Mandiant identified[10] a campaign by UNC4210, which is suspected to be linked to Turla Team, in which the actors hijacked at least three C2 domains associated with an ANDROMEDA malware botnet. The version of ANDROMEDA associated with the botnet was first uploaded to VirusTotal in 2013 and spread from infected USB keys. After re-registering the expired C2 domains, Turla was seemingly able to use the remaining infections that contacted the servers to profile and select victims (Figure 3).

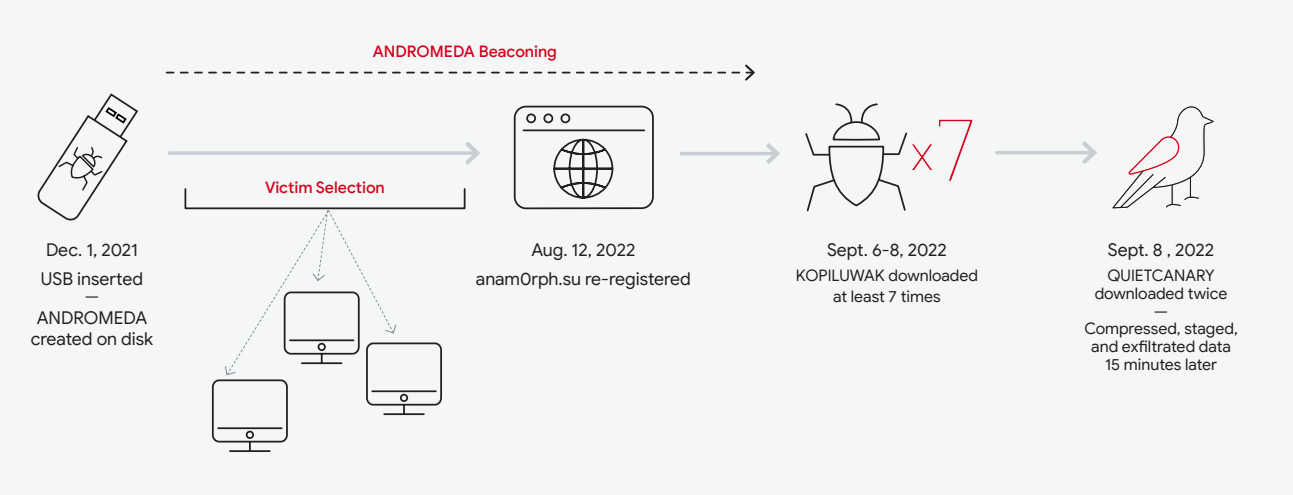

FIGURE 2: Timeline of ANDROMEDA to Turla Intrusion

10. https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

Securing IoT Devices

IoT and smart devices are often not designed to be secure and at times have hard-coded credentials and/or are difficult or impossible to patch when software vulnerabilities are discovered. Organizations actively deploying these devices, or including IoT in digital transformation plans, should ensure that they are able to be properly secured and regularly checked for suspicious activity. Figure 4 outlines security risks related to IoT device manufacturing and operation that asset owners should consider alongside plans to deploy these devices.

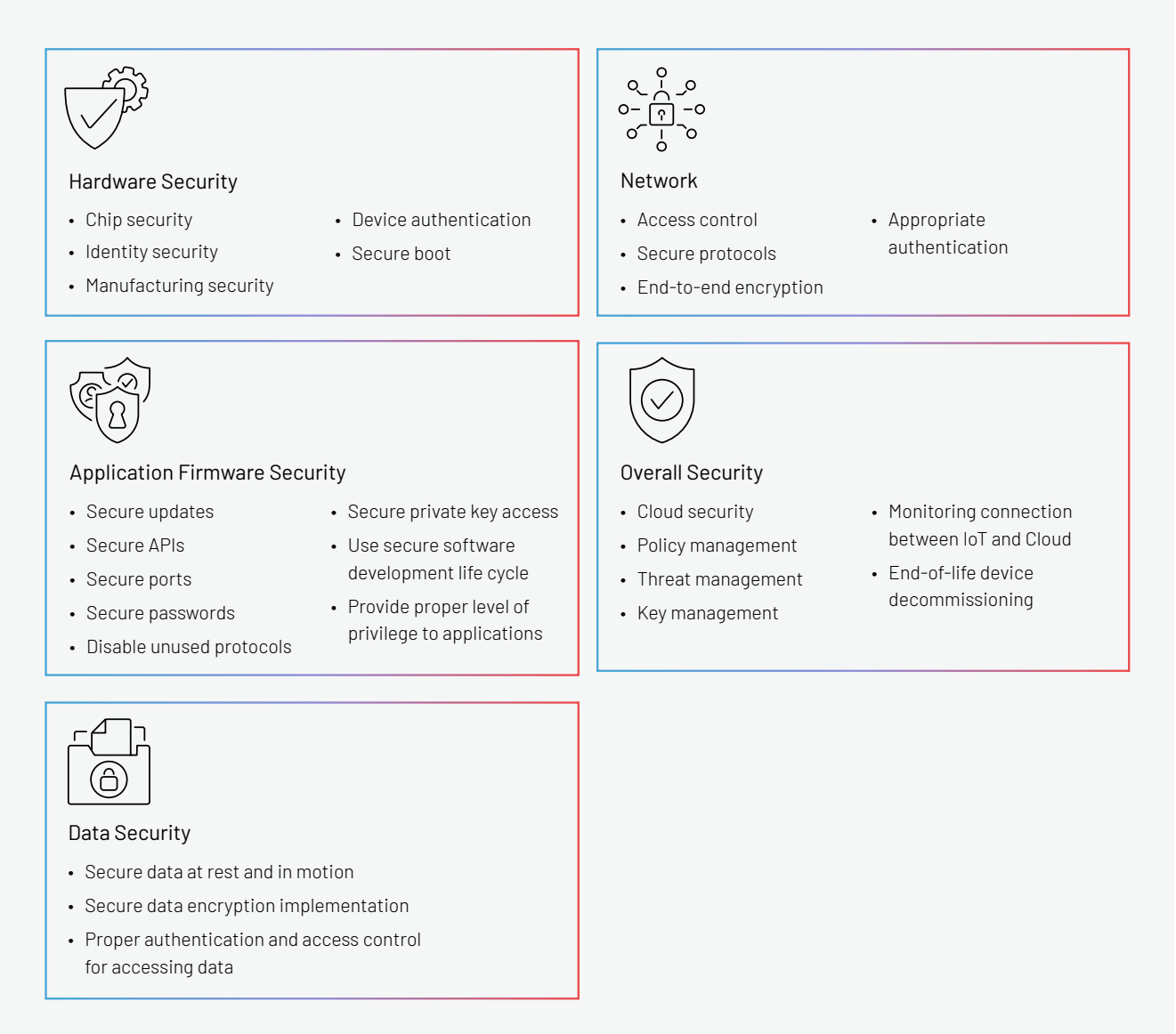

FIGURE 3: Considerations for securing IoT devices

What this means for organizations within a digital transformation

Mandiant anticipates that cyber espionage actors will continue to use this tactic because it provides the attackers with an effective tactical advantage for a relatively low investment of time and resources, as IoT and smart devices are often poorly secured and continue to proliferate. Mandiant also speculates that as IoT and smart devices continue to grow in popularity and tools specifically targeting these devices become more available in underground markets and freely online, espionage actors may show increased interest in use of botnets as a means of disguising intelligence gathering activity as benign or opportunistic, financially motivated cyber crime.

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud