NTT Security

GTIC Monthly Threat Report

February 2019

A Global Threat Intelligence Center
publication from NTT Security

Contents

IoT Devices Continue to Increase Security Risks

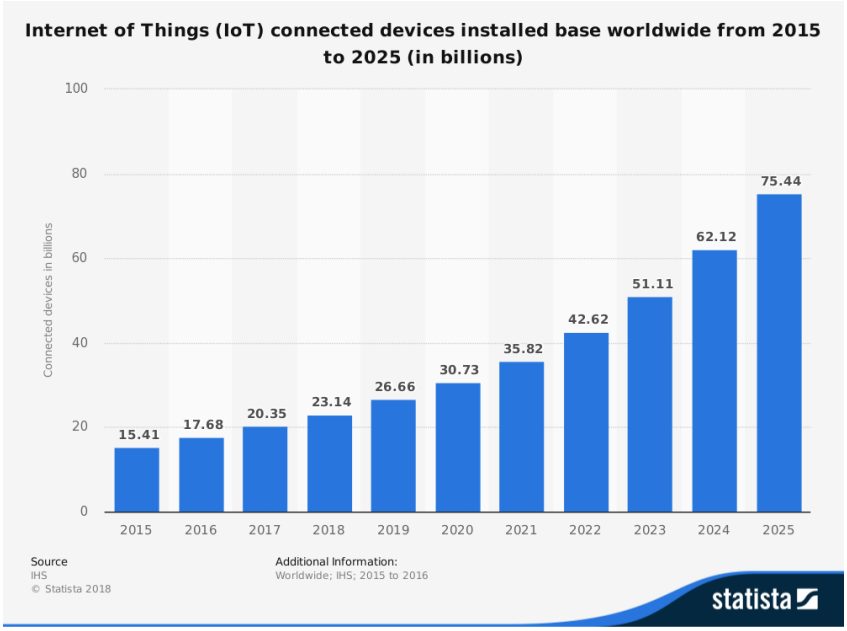
Lead Analyst: Aaron Perkins

Automation often seems like a holy grail for businesses and consumers alike, but we continue learning[1] – automation comes with a cost.

Twelve dollars for a light bulb that can connect to your home Wi-Fi network and be controlled from your mobile device or smart speaker seems a small price to pay for such overwhelming convenience – and it is.

But the Wi-Fi light bulb seems much more expensive[2] when considering it presents another possible entry point into your network. Couple that with the fact that for many IoT devices, security appears to be an afterthought. The IoT industry continues to combat shoddy security practices such as hard-coded passwords and plain-text password storage.

Smart home devices – from security systems[3], to baby monitors[4], to IP-enabled security cameras[5] – all increase security risk in the home, and the same is true in the enterprise environment as well. If it connects to the internet, it potentially increases your security risk.



Conservative predictions foresee the IoT device market reaching over 75.4 billion devices connecting to the internet by 2025, but what are the real risks to adding new devices to your network?

First, just like adding any other device, implementing smart devices into your commercial environment enlarges your digital footprint.

[1] https://arxiv.org/pdf/1812.01597.pdf
[2] https://qz.com/1493748/how-one-lightbulb-could-allow-hackers-to-burgle-your-home/
[3] https://www.forbes.com/sites/thomasbrewster/2016/02/17/simplisafe-alarm-attacks/#92ba8183b002
[4] https://www.huffpost.com/entry/parental-warning-your-bab_n_11668882?ec_carp=5805367622338799240
[5] https://www.detroitnews.com/story/business/2019/02/12/smart-home-devices-like-nest-thermostat-hacked/39049903/

Next, a variety of devices, from thermostats to security cameras, often ship with default configurations which include simple-to-guess passwords. Worse yet, some of these default configurations have passwords such as "admin" or "1234" hard-coded into the device, leaving the end user with no method of securing that device.

More smart devices connecting to your network mean more management challenges.

Additionally, more smart devices connecting to your network mean more management challenges – patching, testing and pushing security updates, and monitoring. What makes this even worse is that many of these devices have no upgrade or patch plan.

A determined attacker, once inside your network, may seek to move laterally through the network to access proprietary company information, credit card data, customer data, and other valuable assets within the environment.

Fortunately, there are steps you can take to help secure your environment before IoT devices increase your security risk.

- Take your time when selecting smart security devices or any IoT device.

Understand the configuration of the device before connecting it to your network and consider vulnerability assessment and penetration testing activities on your environment both before and after connecting your device(s).

- Change all default username/password configurations on smart devices.

If the smart device you are considering introducing into your environment uses hard-coded credentials such as password and login information, NTT Security recommends not connecting the device to your network.

Many IoT devices ship with default credentials. Ensure you modify the default credentials to ensure the device remains secure.

- Use the 'least privilege' access model.

If the device passes the previously mentioned security measures and you decide to connect the device to your network, ensure those personnel granted access to the device and its configuration are the only ones who genuinely need to have access.

- Have an incident response (IR) plan prepared in the event your devices are compromised.

At a minimum, your IR plan should include the steps your organization will take to contain the incident, should identify who oversees leading the response effort, and should clearly outline what your mitigation steps will be to reduce the impact of the incident.

Make no mistake – NTT Security advocates a measured approach to IoT implementation. In fact, NTT DATA was just recognized by Everest Group as a 'Leader' in the group's *IoT Services PEAK Matrix™ Assessment 2019*[6], and NTT Security is proud to be delivery partner of NTT DATA.

[6] https://us.nttdata.com/en/news/press-release/2019/february/ntt-data-recognized-as-a-leader-in-everest-groups-iot-services-peak-matrix-assessment-2019

Iran Expected to Increase Cyber Espionage – And Why That Matters

Lead Analyst: Aaron Perkins

In a rather expected move, the European Union recently imposed sanctions on Iran in response to Iran's ballistic missile tests, as well as the country's assassination plots in Europe. These new sanctions levied toward Iran come on the heels of the November 2018 arrest of two Iranians for the SamSam ransomware campaign, which wreaked havoc around the world.[7]

The sanctions will force Iran – a country which finds much of its revenue from petroleum – to ensure growth in non-oil industries, and the fastest way to grow those other industries is, according to the NCSC, "penetrate U.S. networks for economic or industrial espionage purposes."

Iran also has a history of attacking industries which provide stability to a nation's or region's economy, and in 2018, the U.S. National Counterintelligence and Security Center (NCSC) noted Iran is indeed an increasing cyber threat. [8]

The European Union Agency for Network and Information Security (ENISA) says this move will likely lead Iran to increase state-sponsored cyber-espionage "in pursuit of its geopolitical and strategic objectives at a regional level."[9] In other words, Iran will likely be ratcheting up the intensity, frequency, and lethality of cyber-attacks in the coming months.

Iran will likely be ratcheting up the intensity, frequency, and lethality of their cyber-attacks in the coming months.

Intelligence reports[10] indicate there is at least one Iranian nation-state sponsored advanced persistent threat – APT 39 – which focuses cyber espionage efforts on stealing personal information. APT 39's mission is different than what Iran has historically been known for when it comes to hacking.

In contrast to China's typical hacking goal of stealing novel technical information, and Russia's hacking goal of mapping networks and implanting backdoors for persistence and future access, Iran has a history of hacking with the goal of causing as much destruction as possible.

If this plays out as predicted, Iran will quickly join the ranks of China and Russia as the 'most capable and active cyber actors tied to economic espionage.' What this means for you and your organization is that the threat of having your data stolen, your systems destroyed, or your network compromised increases even more.

This is especially true for those organizations in critical infrastructure sectors around the globe, as Iran has a history of attacking critical infrastructure, primarily for the purposes of causing as much damage as possible.

Still have unpatched software and hardware? Harden your defenses by patching those security vulnerabilities.

Still have a lax BYOD security policy? Enact stricter measures when devices connect to your network.

Haven't yet updated the IoT/OT devices throughout your organization? It's time.

[7] https://wp.nyu.edu/compass/2018/11/13/iranian-cyber-warfare-state-repression-and-international-retaliation/
[8] https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf
[9] https://www.haaretz.com/middle-east-news/iran/eu-agency-iran-likely-to-boost-cyber-espionage-efforts-as-ties-with-west-worsen-1.6878129
[10] https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

Significant Vulnerability

Lead Analyst: Jose Hernandez

During February, GTIC researchers noted many new vulnerabilities impacting a wide variety of systems and applications, but the most notable was a recently discovered vulnerability in an open-source application.

RunC Container Escape Vulnerability

Threat Status: High

CVE-2019-5736[11]

Severity: High (CVSS: 7.2)

Date: 11 February 2019

Remediation Details: Patches have been released to address this vulnerability.

Affected Versions:

- Docker 18.9.1
- Docker 1.12.6
- Docker 1.12
- Docker 1.6.1
- Docker 1.6
- Docker 1.3.3
- Docker 18.09
- Docker 18.06
- Docker 17.05
- Docker 17.04
- Docker 17.03
- Docker 1.8.3
- Docker 1.4.1
- Docker 1.3.2
- Docker 1.3.1
- Docker 1.3.0
- Docker 1.12.3
- Docker 1.12.2
- Docker 1.0.0

Analyst Note: Security researchers recently discovered a vulnerability[12] which affects the runC portable container runtime software. The open-sourced runC software has many applications and is an important component of numerous other pieces of container software such as Docker.

The vulnerability allows an attacker to overwrite the host runC binary. By overwriting the runC binary in the host system, the attacker gains root-level permissions and can execute arbitrary code on the underlying host system. An attacker can exploit the vulnerability with a new container controlled by the attacker or an existing container to which the attacker can write.

The vulnerability lies in the way the runC binary interacts with the process file system of the container. The security researchers discovered that by tricking runC into executing the */proc/self/exe*, which is a *symbolic* link to the runC binary, they could execute code on the host. The attacker must have root-level permissions on the within the container in order to successfully exploit this vulnerability, and public exploit code is available to exploit this vulnerability.

[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5736
[12] https://seclists.org/oss-sec/2019/q1/119

NTT Security Observations

Lead Analyst: Terrance DeJesus

In February, GTIC researchers reviewed NTT Security vulnerability data. For this analysis, the goal was to analyze the most targeted Common Vulnerabilities and Exposures (CVEs) and the attacker patterns and intrusion sets associated with the campaigns using these CVEs. Researchers also attempted to identify additional tactics within these campaigns. And, while these additional tactics may not be heavily used in terms of overall volume, they were still being leveraged for one-off campaigns.

Security Warning Concerning Xiongmai Products

With Mirai code publicly available, attackers and developers created many variants, keeping much of the original source code intact. During February, GTIC researchers identified a Mirai variant being installed on Xiongmai IoT devices, specifically IP cameras and DVRs. This campaign targeted CVE-2017-7577, a vulnerability in the Xiongmai *uc-httpd* service allowing remote code execution via custom HTTP requests.

Xiongmai has a history of producing IoT devices with little-to-no security, and Xiongmai devices have been associated with Mirai before, all the way back to 2016 when Mirai first appeared.

Security firms around the globe have taken notice[13], confirming the lack of security inherent in Xiongmai devices and components. Security researchers continue attempts to fix the vulnerabilities present in these devices, with device types ranging from DVRs, to NVRs, to video surveillance equipment, and more.

GTIC researchers assess threat actors will conduct more reconnaissance via internet-wide scanning, attempting to locate IoT Xiongmai devices and Xiongmai components within other IoT devices. Once these devices and components are discovered, attackers will likely exploit the devices and install IoT malware or leverage the devices as part of a botnet.

New SMB Vulnerability: CVE-2019-0630

On 12 February 2019, a remote code execution (RCE) vulnerability in Microsoft Server Message Block 2.0 (SMBv2) was published. If successfully exploited, the vulnerability could allow an attacker to remotely execute code on the vulnerable server by a specially crafted packet because of how SMBv2 handles certain requests.

Vulnerable SMB servers always pose as a significant threat to an organization. ETERNALBLUE and DOUBLEPULSAR, which wreaked havoc on vulnerable devices in 2017, are perfect examples of what can happen with vulnerable SMB servers.

GTIC researchers have only noticed a small amount of exploit attempts against this specific vulnerability and are continuing analysis. NTT Security recommends applying the following Microsoft patch:

Microsoft Patch: msft-kb4486564-11fbac8f-a728-4e04-8372-8cddd6574ab0

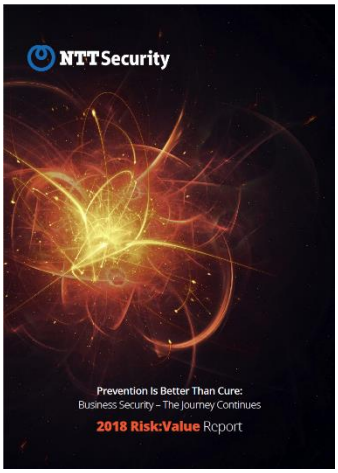
[13] https://sec-consult.com/en/blog/2018/10/millions-of-xiongmai-video-surveillance-devices-can-be-hacked-via-cloud-feature-xmeye-p2p-cloud/

Conclusion

So far in 2019, GTIC researchers have noticed attackers targeting IoT device vulnerabilities in botnet campaigns, internet-wide scanning, and blind hacks. The increase in network-connected devices in both residential and commercial settings continues to broaden the threat landscape. These vulnerable devices, often left out of asset security management plans, are easy targets for threat actors who can find publicly available vulnerabilities and exploit code to target them.

Manufacturers' choice to focus more on creating the greatest number or products for the lowest cost without implementing secure coding practices leaves a market full of insecure devices available across the globe. Many of these devices are vulnerable in the source code, and most are built at such low quality that they cannot support essential functions such as communication encryption. Besides applying a layered-defense approach, taking the time to review IoT products and the manufacturers behind the components will help your organization make better decisions before purchasing and implementing IoT devices into your network environment.

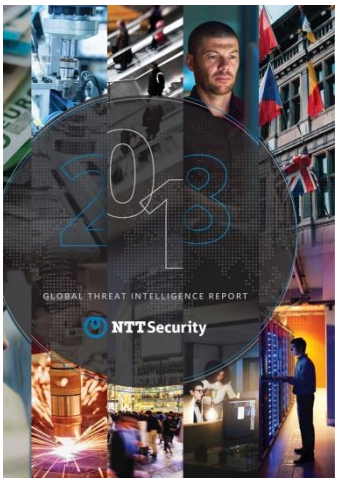
NTT Security Annual Reports



Risk:Value 2018

Many organizations are stuck in a reactive mindset when it comes to information security and would opt to pay a hacker's ransom rather than proactively invest in security. That's a key finding in this year's Risk:Value 2018 Report.

Download your copy today!



2018 Global Threat Intelligence Report

This year's report summarizes activity we detected in over 6.1 trillion+ logs and more than 150 million+ attacks, along with vulnerability scans, incident response engagements, and diverse findings from threat research and threat intelligence teams across NTT Security.

Download your copy today!

About GTIC

The NTT Security GTIC protects and informs NTT Group clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures, threat reports and white papers, visit the resource page on www.nttsecurity.com or our blog.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.