REVOLVING AROUND
YOUR OPERATIONS

NSFOCUS

CODY MERCER
SENIOR THREAT INTELLIGENCE RESEARCH ANALYST

AGENDA

01 Introduction

02 What’s An IoT Device?

03 Phases of GTM Vulnerable IoT Devices

04 Real-World Examples of Cyber Attacks Involving IOT Devices

05 Best Practices & Security Measures

06 Key Takeaways

WHAT IS AN IOT DEVICE?

What is an IOT Device – Anything with an IP/MAC Address

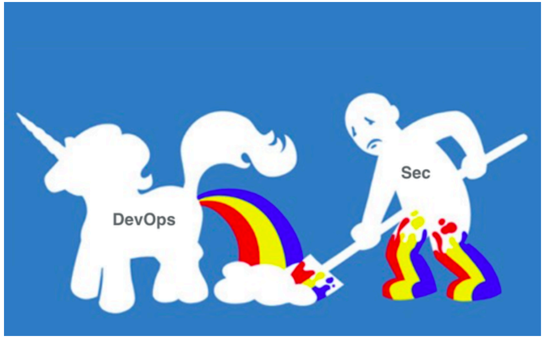
- Smart Cars/Drones
- Cameras/Video Records
- Televisions/Security Cameras/DVRs
- Gaming Platforms
- Air Conditioning Systems/Talking Refrigerators/Electric Meters
- Smart Phones/Watches/Fitbits
- Health Care Devices (Heart Monitors, Pace Makers, Defibrillators, Insulin Pumps)

ALARMING STATISTIC

“The U.S. Department of Homeland Security (DHS) states that 90% of security incidents result from exploits against defects in software. That's a big statement - and it implies that poor software development may be the biggest cyber threat of all.”

REFERENCE: *Is poor software development the biggest cyber threat?* (September 2015)
http://www.csoonline.com/article/2978858/application-security/is-poor-software-development-the-biggest-cyber-threat.html

Vulnerable IoT Lifecycle – Cost Effective & ROI



- ❖ **R&D -** *"It is not in our budget or included in the SDLC at the moment"*
- ❖ **Production & Operations** – *"We don't not have the proper SAST/DAST or tools necessary to apply security requirements"*
- ❖ **Sand-Box & Testing** – *"Your implemented security protocols is affecting our regression testing and latency baselines"*
- ❖ **Integration** – *"Your security stack is not cooperating with other applications we had to lose Info Sec"*
- ❖ **Go Live** – *"Sorry we had to meet our project milestones and had to drop 75% of your security requirements to meet objectives"*
- ❖ **Deployment** – *"We have been hacked"*

Deployment – COTS & GOTS (Commercial/Government Off the Shelf)

- Users unaware of needed patch/firmware update requirement
- Un-patched systems and O.S's - No longer created or out of circulation (.i.e. XP)
- Default passwords remain unchanged
- Unnecessary open ports and/or un-secure applications permit for easily compromised asset

PHASE THREE – Why Vulnerable?

Scanning & Reconnaissance

- Scanning conducted to identify unpatched systems & unneeded open ports
- IoT IP devices owned and compromised
- Script kiddies easily develop scripts that conduct scanning capabilities
- Easily obtained malware from darknet database repositories

CTF - Owning Device

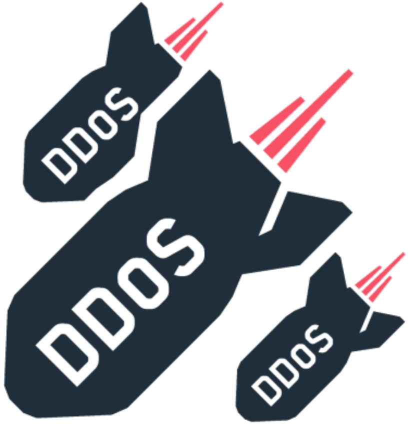
- Backdoors created for ex-filtration purposes
- RAT (Remote Access Trojans) installed and remain sleepers
- Assist in bot armies in DDoS attack campaigns
- Assist in RaaS (Ransomware as a Service) campaigns
- Assist in DaaS (DDoS as a Service) campaigns
- Serve as proxies to facilitate in larger attack campaigns

PREVIOUS COMPROMISED IOTs?

- **iPhone/Android & Phone Apps -** NightSkies (3G running iOS 2.1), Driodjack (Droid), SideStepper (iOS)
- **Macbooks** – DarkSeaSkies (CIA)
- **EFI Firmware of MacBook Air -** DarkMatter, SeaPea, NightSkies (CIA)
- **Dahua Video Cameras -** Attacker can access the user database of a Dahua camera without needing administrative privileges and extract the user name and password hash
- **Drones -** (Parrot AR.Drone 2.0, Parrot Bebop, DJI Phantom 1/2/3/4, DJI Inspire, DJI Mavic, Yuneec Brezee, Yuneec Thypoon, Yuneec Tornado)
- **Samsung TVs -** Weeping Angel (CIA) (UNF7500, UNF7000, UNF8000, UNF8500, UNES8000F, E8000GF, UNES7550F)
- **Telsa Model S** – Weak/Faulty Firmware (2016)
- **Jeep Cherokee** – Weak/Faulty Firmware (2015)

MIRAI MALWARE – What is It?

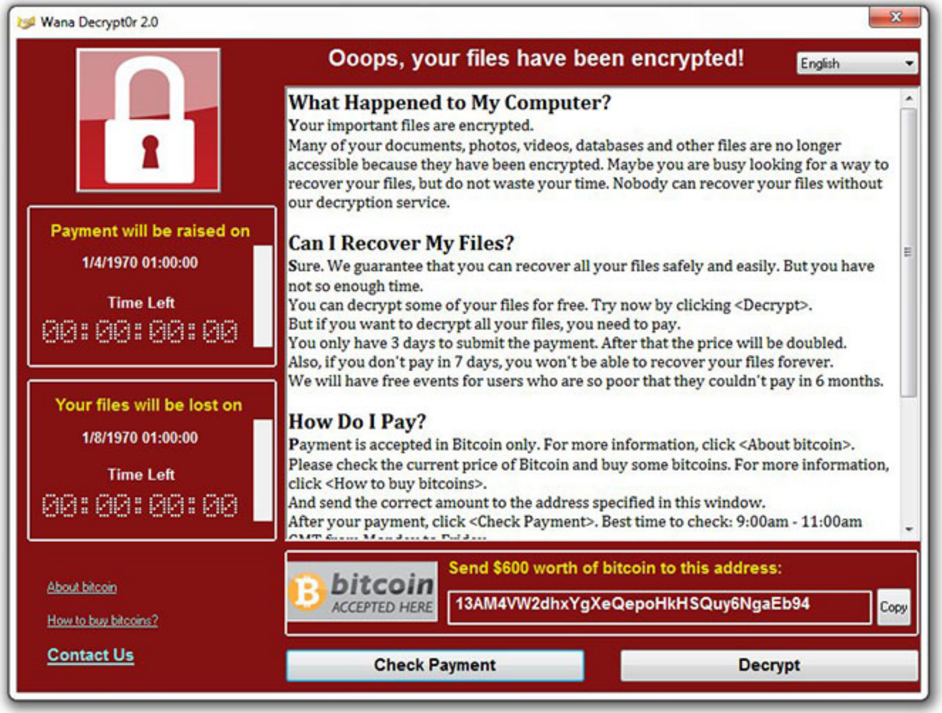
- Mirai works by exploiting weak security on many IoT devices.
- Operates by continuously scanning for IoT devices that are accessible over the Internet.
- Primarily scans for ports **22, 23, 5747**, etc. that are open, and can easily be configured to scan for others.
- Once connected to an IoT, Mirai attempts to login, gain access, and infect the device.
- The infected device then scans other networks looking for more IoT devices and launches DDoS attacks.



WANNACRY RANSOMWARE ATTACK

This Just In: I #WannaCry

- Exploits the **ETERNALBLUE SMB** vulnerability or **DOUBLEPULSAR** backdoor for propagation and infection of the ransomware.
- Ransomware sample contains three Bitcoin wallets provided by the attacker.



Ooops, your files have been encrypted!

Payment will be raised on

1/4/1970 01:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 01:00:00

Time Left

00:00:00:00

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

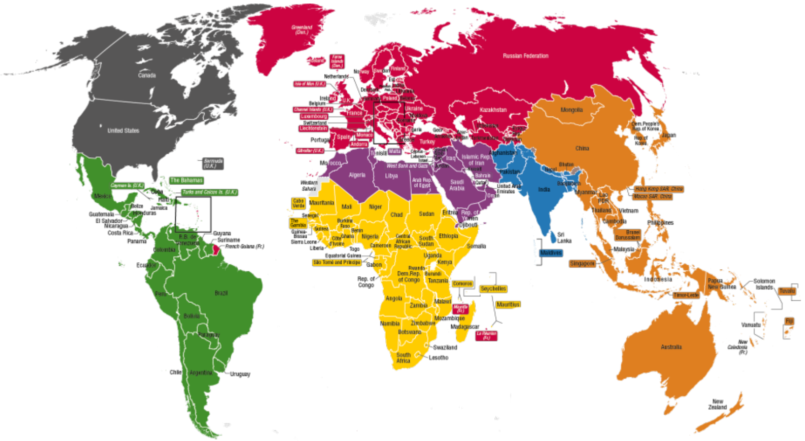
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

RANSOMWARE WANNACRY IMPACT



Largest ransomware attack in history

1. 200+ countries affected
2. Hitting all major sectors to include medical, industrial, financial
3. More than 200,000 assets compromised
4. Variants to the strain rapidly developed within hours of identification and patch release
5. Attack methods include phishing, spamming, capitalizing on Microsoft vulnerability CVE-2017-044
6. Financial loss world-wide reported a little under 1-Billion U.S dollars
7. Tools used in exploit were supposedly developed by NSA’s hacking crew the ‘Equation Group’
8. Attacks are often state-sponsored with limitless resources and funding

NSFOCUS THREAT INTELLIGENCE REPUTATION & TI PORTAL

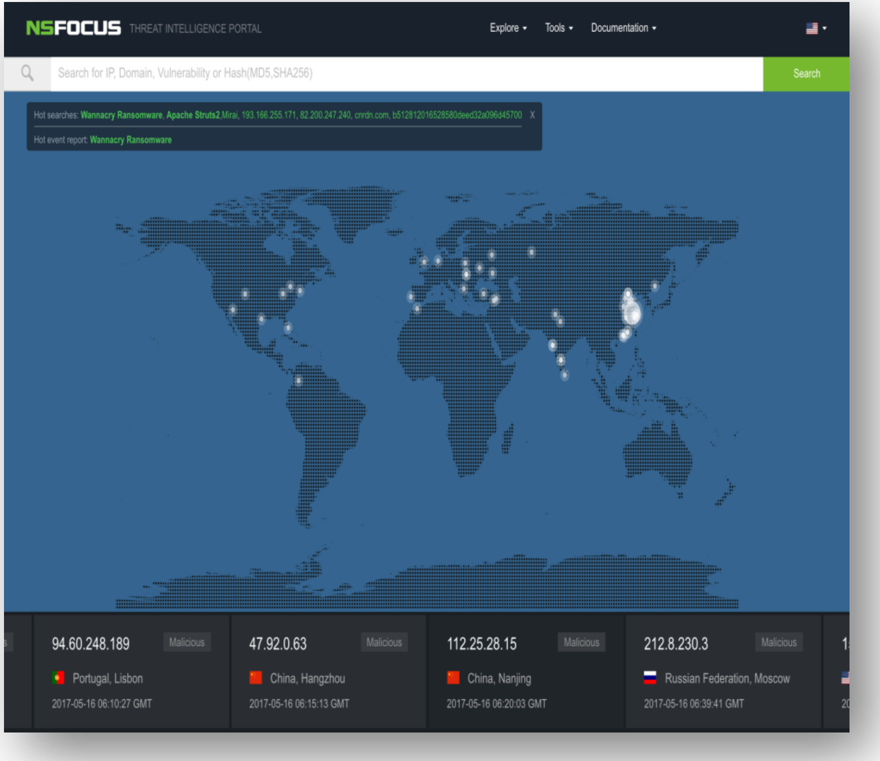
❖ IP/URL/C2 Reputation Data

❖ Threat Campaigns/Actors

❖ Malware Analysis

❖ Hash Value Review

❖ Strategic/Tactical Intel


NSFOCUS THREAT INTELLIGENCE PORTAL
Explore ▾
Tools ▾
Documentation ▾
Search for IP, Domain, Vulnerability or Hash(MD5,SHA256)
Search
X
Malicious

Hot searches: Wannacry Ransomware, Apache Struts2,Mirai, 193.166.255.171, 82.200.247.240, cnrdn.com, b512812016528580deed32a096d45700

Hot event report: Wannacry Ransomware

94.60.248.189 Malicious
Portugal, Lisbon
2017-05-16 06:10:27 GMT

47.92.0.63 Malicious
China, Hangzhou
2017-05-16 06:15:13 GMT

112.25.28.15 Malicious
China, Nanjing
2017-05-16 06:20:03 GMT

212.8.230.3 Malicious
Russian Federation, Moscow
2017-05-16 06:39:41 GMT

SPECIFIC REPUTATION PROTECTION MEASURES

- Permits for upload into various NSF and 3rd-Party security appliances
- List of active C2 servers prevents potential botnet army DDoS attacks
- Prevents internal users from accessing malicious servers
- Blocks known servers hosting malicious activity to include spear-phishing campaigns and/or malware repository databases

WHAT YOU CAN DO TO PROTECT YOUR SYSTEMS

- **Change/Configuration Management** - Ensure that all your IoT, software, firmware, and applications are patched and up to date

- **Network Security** - Use commercial or open source TI to block your organization’s access to malicious C2/IP/URL addresses

- **Ransomware** - Keep multiple backups that are encrypted in more then one location with encryption keys in separate locations

- **Threat & Vulnerability Management** - Change default passwords

- **Mandatory Training** - Continuous employee cyber-security awareness training either quarterly or bi-annually

KEY TAKEAWAYS

- The IoT SDLC (Solution Development Lifecycle) & deployment process is a precarious industry that poses exceptional danger to all IP entities on a global scale
- Owners of the compromised IoT device are often unaware that they are a contributor to an illegal operation
- Continuous access to updated reputational data can significantly increase your protective measures in-depth/in-breadth within your infrastructure

NSFOCUS

Thank You

Phone: 210-246-2787

Email: cody.mercer@nsfocusglobal.com