THREAT BRIEFING

Current APT Activities

Daniel dos Santos, PhD
Head of Security Research
Agenda

1. Data overview – risk & threats
2. Deep dive into APT trends
3. Conclusion
1. Data overview
How we collect data

1. Telemetry upload
2. Threat enrichment
3. Threat Intel Generation
4. IoCs, Threat Reports, Feeds

Forescout Customer Networks (opt-in data sharing)

https://www.forescout.com/research-labs/
Vedere Labs Threat Intelligence is based on millions of devices and billions of data points that include device configuration and network behavior at more than 1500 sites globally.

We compute the risks for millions of devices by considering multiple factors, including CVEs, exploitability, misconfiguration and misbehavior.

We monitor the impact of industry threats & vulnerabilities (e.g., Log4Shell) over time.

https://dashboard.vederelabs.com/
Network risks

- Data from **18+ million devices** on customer networks
  - 24% of devices are **non-IT**
  - **Major attack surface** that is growing and being targeted by threat actors

- Riskiest devices are
  - **IT: network infrastructure** (e.g., routers and firewalls), one of the main initial access points for ransomware and other actors
  - **IoT: surveillance** (e.g., IP cameras and NVR) and **VoIP**, lots of easily exploitable vulnerabilities and Internet exposure
  - **OT: building automation** (e.g., HVAC and access control), critical impact and often Internet connectivity
APT origins and targeted sectors

- Data from **malicious DNS requests** detected on our customer networks
  - Close to 20 APTs and more than 300 malicious domains seen

- Top observed **APTs in 2022:**
  - **APT29 / COZY BEAR** – Russian state-sponsored (SVR)
  - **IcedID / LUNAR SPIDER** – Russian/Eastern European cybercriminals targeting Financial Services
  - **Evil Corp / INDRIK SPIDER** – Russian/Eastern European cybercriminals targeting several sectors
APT motivations and TTPs

- Two major types of APTs with almost equal split of activity:
  - **Cybercrime** – ransomware and financial scams (BEC, phishing)
  - **State-sponsored** – espionage and destructive malware

- Top TTPs are traditional **Windows-based exploitation**

APT activity by group motivation

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>T1078 - Valid Accounts</td>
</tr>
<tr>
<td>Execution</td>
<td>T1059.001 - PowerShell</td>
</tr>
<tr>
<td>Command and Control</td>
<td>T1071 - Application Layer Protocol</td>
</tr>
<tr>
<td></td>
<td>T1573 - Encrypted Channel (HTTPS)</td>
</tr>
<tr>
<td>Discovery</td>
<td>T1082 - System Information Discovery</td>
</tr>
<tr>
<td></td>
<td>T1057 - Process Discovery</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>T1053.005 - Scheduled Task/Job</td>
</tr>
<tr>
<td>Collection</td>
<td>T1074.001 - Data Staged: Local Data Staging</td>
</tr>
<tr>
<td></td>
<td>T1560 - Archive Collected Data</td>
</tr>
<tr>
<td>Exfiltration</td>
<td>T1041 - Exfiltration Over C2 Channel (HTTPS)</td>
</tr>
<tr>
<td>Impact</td>
<td>T1486 - Data Encrypted for Impact</td>
</tr>
</tbody>
</table>

Source: [https://www.scythe.io/library/threat-thursday-top-ransomware-ttps](https://www.scythe.io/library/threat-thursday-top-ransomware-ttps)
Attack attempts on exposed vulnerable services

- Main observed techniques on **Adversary Engagement**:
  - T1190 – **Exploit Public-Facing Application** – known vulnerabilities such as EternalBlue, Log4j
  - T1078 – **Valid Accounts** – default credentials for IoT devices
  - T1071 – **Application Layer Protocol** – HTTP and others for C2 and exfiltration

- These attacks include a **third threat actor type: hacktivists**
  - Adversaries **compromising devices** to use as tunnels or botnets for DDoS

- Attacks originating mostly from **American and Asian IP addresses**
  - Attackers often using **proxies, VPNs and Tor** exit nodes

- Attack attempts by country of origin (IP address)
  - United States: 40%
  - China: 18%
  - Cambodia: 13%
  - Germany: 5%
  - United Kingdom: 5%
  - Japan: 4%
  - South Korea: 4%
  - Russia: 4%
  - Singapore: 3%
  - India: 4%
  - Japan: 4%
  - United States: 40%
  - South Korea: 4%
  - India: 4%
  - Russia: 4%
  - Singapore: 3%
  - United States: 40%
  - South Korea: 4%
  - India: 4%
  - Russia: 4%
  - Singapore: 3%
2. Deep dive into APT trends

https://www.forescout.com/threat-briefings/
Ransomware evolution

- More than **4000 publicly tracked incidents** in the past couple of years ([https://darkfeed.io/](https://darkfeed.io/))
  - US top targeted country with more than 700

- Hundreds of active groups, many using the RaaS model
  - Lockbit and Conti the most active

- TTPs evolved from data encryption to multi-faceted extortion attacks
  - Exfiltration, denials of service, public shaming

- Evolution of the ransomware landscape is far from over. Adversaries changing because of:
  1. Proliferation of IoT/OT devices
  2. State-sponsored ransomware

*Example: ALPHV exploiting unpatched network infrastructure, releasing sophisticated encryption software and targeting virtualization servers
Ransomware and IoT/OT

**Conti:**
- Affiliates relying on **common TTPs** (such as initial access via stolen or weak RDP credentials, execution via PowerShell and lateral movement via Windows vulnerabilities) **mixed with IoT exploits**
- Leaked internal **documentation and chats advocate for the use of IoT devices as entry points, since they are often unpatched.**
- Also encouraged their affiliates to **leverage botnets** with dormant infections on IoT equipment. [https://www.forescout.com/resources/analysis-ofconti-leaks/](https://www.forescout.com/resources/analysis-ofconti-leaks/)

**Other examples:**
- **DeadBolt, Qlocker, Checkmate** targeting Internet-exposed and local **NAS devices**
- Ransomware groups targeting CVE-2022-29499 on **Mitel VoIP devices** for initial access
- **Trickbot** (frequently used to drop ransomware) abusing **MikroTik Routers** as C2 Proxies
- **EKANS** targeting **OT processes** in 2020

"CISA and FBI have observed Conti using Router Scan to maliciously scan for and brute force routers, cameras, and network-attached storage devices" [https://www.cisa.gov/uscert/ncas/alerts/aa21-265a](https://www.cisa.gov/uscert/ncas/alerts/aa21-265a)
“State-sponsored ransomware”

- Ransomware is getting **increasingly mixed with state-sponsored activities.** Examples:
  - **Conti** publicly taking Russia's side in the ongoing war, then crippling and promising to topple the Costa Rican government
  - **Chinese threat actor** Dev-0401 / Bronze Starlight using several similar ransomware families (LockFile, AtomSilo, Rook, Night Sky, and Pandora) against targets across the world since mid-2021 in a campaign believed to be a disguise for espionage. This actor
  - **North Korean actors** using the Maui ransomware against healthcare organizations

- They often **differ from RaaS groups**, being involved in every stage of an incident and lacking infrastructure for communicating with victims or distributing decryption keys.
  - That's because the ransomware is usually a disguise for other attacks

- “State-sponsored ransomware” is a **growing trend that can lead to larger consequences**, since these actors have the funding and the means to cause greater disruption than exfiltrating or encrypting files
  - For instance, they could focus on **OT targets to cause physical disruption**
State-sponsored malware trends

- **Wipers** used for sabotage, as part of cyberwar, or for destruction of evidence
  - Sometimes **disguised as ransomware** to mislead incident response or hide motivations
  - Overwriting or encrypting files, overwriting MBR/MFT
  - Typically used on IT systems, but recently **AcidRain used to wipe SATCOM modems in Ukraine**

  ![Message left by WhisperGate after reboot](image)

- **OT/ICS malware** continues to abuse insecure-by-design native capabilities of OT equipment
  - **Industroyer2** leveraging OS-specific wipers and a dedicated module to communicate over the IEC-104 protocol for electrical substations
  - **INCONTROLLER** toolkit with modules to read/write from/to ICS devices using industrial network protocols, such as OPC UA, Modbus, CODESYS, and Omron FINS

- **Botnets:** Cyclops Blink developed by Sandworm as a possible successor to VPNfilter. Taken down soon after discovery, but active since 2019
  - Targeted WatchGuard and ASUS routers
Hacktivism

- More than **100 groups** have conducted cyberattacks since the beginning of the Russian invasion of Ukraine
  - Mostly **DDoS**, but also data breaches, wipers and distributing propaganda
  - Some **attacks on critical infrastructure**: e.g., EV chargers in Moscow
  - Currently more than 70 active groups, located mainly in Russia or Ukraine but also in Belarus, Turkey, Romania, Poland, Portugal and Italy
  - Coordination and the communication of their actions usually happens via **Twitter or Telegram**

- **Killnet** became notorious using simple DDoS tools to take down websites of critical infrastructure companies in US/Europe
  - Targeted airports, banks, gov. agencies and others
  - Also spread propaganda to more than 100,000 members of their Telegram channel
  - Several attacks detected on our honeypots brute forcing credentials on FTP, HTTP/S, and 22
3. Conclusion
Mitigation

Why it is possible

- Attacks are **not immediate and fully automated**. Dwell time changes per attack type but it's typically at least a week
- **Cybercrime-as-a-service** means that there are up to *hundreds* of very similar attacks happening simultaneously
- Most **tools and techniques used are well-known**. Except in the case of some state-sponsored malware

Recommendations

- Extend visibility, monitoring and patching to **IoT and network infrastructure** devices
- Plan for **virtualization and storage servers** as main targets – i.e. backup VMs and server infrastructure
- Monitor **activity in dark nets** for hacktivist behavior
- Invest in **DDoS protection** via CDNs, load balancers, web application firewalls, etc
- **Hunt for threats** in networks using known TTPs more than any specific IoC
- **Segment** the network in a way to isolate IT, IoT and OT. Limit network connections to only specifically allowed devices.
- Use **OT-aware DPI-capable monitoring** to alert on malicious indicators and behaviors, watching internal systems and communications for known hostile actions.
Takeaways

- **Attack surface increasing**: IoT, OT, network infrastructure, virtualization servers, ...

- Cybercrime, hacktivists and state-sponsored actors are all leveraging this increased attack surface

- Mitigation should be based on threat intelligence and prioritize the increased attack surface
References

- Dashboards: https://dashboard.vederelabs.com/

- Technical Threat Reports: https://www.forescout.com/threat-briefings/
  - Industroyer2/Incontroller

- For more info contact us at vederelabs@forescout.com
Thank you.