K logix

BE CONFIDENT.

VOL 2 | OCTOBER 2022 | THREAT INTEL NEWSLETTER

Internet of Things (IoT) and Phishing as a Service (Phaas)

C-Suite level threat review by applicable business area addressing active threats.

IoT threats are rapidly growing. According to Gartner, they predict “by 2025, 73.1ZB of data will be generated by IoT.” This massive influx of data needs unique security solutions to prevent threat actors from leveraging IoT vulnerabilities such as botnets and open ports. In addition, Phishing as a Service allows people to purchase packages such as EvilProxy on the darknet to bypass two-factor authentication (2FA) and infiltrate environments.

IoT (Internet of Things) Botnets

A Botnet is a network of computers infected with malware that threat actors can control without the system owners' knowledge. These sometimes send spam messages or execute a Distributed Denial of Service (DDoS) Attack. DDoS intentionally paralyzes a computer network by flooding it with data sent simultaneously from many individual systems, such as smart cameras, can and have been compromised, building powerful botnets of many devices.

PhaaS (Phishing as a Service)

Mandiant discovered a new PhaaS platform called Caffeine, where cyber criminals purchase tools similar to EvilProxy. EvilProxy steals session cookies and bypasses 2FA through reverse proxy and cookie injection methods. According to Resecurity Inc., the kit can steal valid session cookies from targeted machines and bypass the need for users to authenticate their credentials, such as usernames, passwords, or 2FA tokens allowing access to the environment.

IoT Botnets

Threat Level: Medium

Attack:

IoT Botnets target many types of devices. The malware scans the internet for devices with open ports and then downloads itself, which becomes a scanner for more botnet operators. Numerous botnets are resurfacing, including new versions of Mirai, one of the largest on record. Threat actors are harnessing the capabilities of the old Mirai botnet to build more recent versions, and several are currently active.

Remediation:

- Establish a baseline of network and IoT devices (asset management)
- Update the firmware with latest patches and releases (cyber hygiene)
- Use tools to scan for IoT devices that automate detection, updates, and patching
- Group similar devices within secure zones or software-defined perimeters for tighter visibility and governance over each

PhaaS

Threat Level: High

Attack:

EvilProxy, the PHAAS mentioned above, steals account login credentials by deploying a payload, called JuiceStealer. EvilProxy leverages supply chain attacks to gain access to development libraries like GitHub. Threat actors target these libraries because they provide access to other targets. End users of GitHub download the software packages assuming they are safe when in truth, they may contain malware.

Remediation:

- Security Awareness training prepares the users for phishing and other social engineering attacks and teaches them how to respond to avoid loss of information and reputation to the organization.
- Scanning code repositories mitigates vulnerability to the sup-

Botnet Mitigations

- Generate rich and dynamic context around every connected IoT device by collecting device information
- Perform accurate policy control
- Minimize the organization’s exposure to potential device-level risks
- Continuously monitor the connected devices for anomalies and unauthorized access

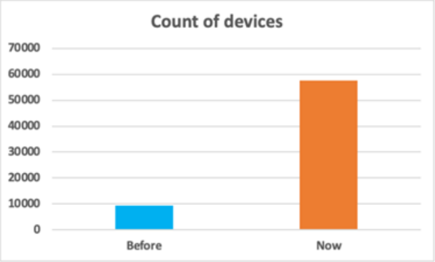
PhaaS Mitigations

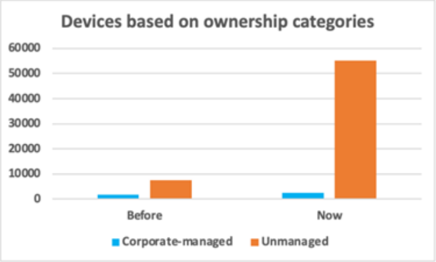
- Cyber awareness training to address manipulation attempts by attackers to mitigate the risk of phishing
- Social engineering mitigation training
- Automated training through a tool is a way to education users in a scheduled manner
- Secure code repository procedures

How K logix Can Help

- Technology Advisory
  - Tools that mitigate botnets and identify IoT devices on the network
  - Security awareness automation
- Programmatic Advisory
  - Asset Management for IoT with policies and procedures
  - Initial build out of the security awareness program

Charts by Netskope on IoT





Threat actors keep finding new ways to infiltrate IoT devices every day, and the trend will continue to accelerate as IoT solidifies its presence in mainstream business use.

Targets of EvilProxy from Recorded Future

EvilProxy disseminates phishing campaigns to compromise consumer accounts from well-known brands such as:

- Apple
- Facebook
- GoDaddy
- GitHub
- Google
- Dropbox
- Instagram
- Microsoft
- Twitter
- Yahoo
- Yandex

ABOUT K LOGIX

Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.