K logix

BE CONFIDENT.

VOL 1 | SEPTEMBER 2022 | THREAT INTEL NEWSLETTER

# Supply Chain Threats: Oktapus & Ragnar Locker

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

In August of 2022, supply chain threats came into focus with the Oktapus campaign. Oktapus hit roughly 130 companies with focused targets in the United States. Nearly 10,000 accounts have been compromised since March of 2022. In addition, malware Ragnar Locker targeted the energy sector with a cyber-attack. The FBI has monitored this ransomware strain since December 2019, and it has a history of breaching over 50 critical infrastructure organizations.

## The Supply Chain Threat:

One threat from the supply chain is an attacker that has used a trusted vendor to infiltrate the target system. A vendor risk management program helps to mitigate supply chain vulnerabilities by vetting vendors for up-to-date compliance and assessments of past breaches. In this example, an attack targeting Okta capabilities on corporate networks resulted in numerous vulnerabilities along the supply chain in 2022. Okta is a multi-factor authentication (MFA)used to secure accounts. The attackers likely gained unauthorized access to secure corporate resources through the Oktapus campaign.

## How Ransomware Works:

Ransomware infects an environment through malicious email or malware, known as droppers. Two of the active droppers this month are Qbot and Emotet. Qbot is a backdoor or information stealer, and can also plant ransomware. Emotet is another piece of malware known to drop ransomware. Emotet is re-emerging this year in new forms that can be purchased on the darknet as a service. Once the ransomware enters an environment, it executes procedures to encrypt information. The victim must pay a ransom to retrieve a key from the threat actor to unencrypt the data.

### Ragnar Locker

**Threat Level: Medium**

Ragnar Locker has been known to target English-speaking countries and critical infrastructure, which includes energy, banking, and healthcare.

**Attack & Remediations:**

- Checks for security products like antivirus and performs mitigations to evade security and backup capabilities by turning off critical services.
- Attempts to connect to removable and mapped drives. This technique is detected by monitoring API calls and newly executed process creation. T1120 (Peripheral Device Discovery)
- Deletes built-in OS data and turns off services that prevent corruption and recovery. T1490 (Inhibit System Recovery)
- Use technical controls to prevent disabling of services or deletion of files involved in system recovery.
- For more technical details see full analysis of Ragnar Locker

### Oktapus Campaign

**Threat Level: High**

Oktapus utilizes phishing techniques to steal Okta identities and two-factor authentication codes to perform supply chain attacks. The motive appears to be financial theft and crypto assets.

**Attack & Remediations:**

- Targets customers on Okta via SMS phishing campaign compromising user credentials and MFA codes. (T1111 Multifactor Authentical Interception)
- This is a social engineering attack utilizing SMS; training and education are the primary prevention mechanisms. Other options include reviewing authorized network devices
- Cloudflare was attacked but not compromised. They recommend using passwordless FIDO2 security keys.
- Another remediation is immediate credential reset.
- For more details see statements by Okta CEO McKinnon

## Ransomware Mitigations

- Manage and reduce the attack surface and keep a current asset inventory
- Behavior-based threat detection tools may detect abnormal activity
- Develop a strong identity and access management program
- If infected by ransom, then restore to the most recent data backup.
- Develop a threat intelligence program to monitor the organization's applicable threats
- Perform frequent security awareness training
- Update software and patch operating systems to prevent vulnerability exploitation
- Follow Zero Trust principles

## Supply Chain Attack Mitigations

- Non-persistence: Delete information as soon as it is no longer needed
- Strict privilege management and privilege-based usage restriction: privileges and information are on a strictly need-to-know basis
- Dynamic privileges, such as restricting access outside work hours
- Social Engineering training, with an emphasis on phishing
- Secure Coding training and practices

## How K logix Can Help

- Technology Advisory:
  - Attack Surface Management
  - Behavior Based Detection
  - Endpoint Detection and Protection
  - Identity and Access Management
  - Threat Management/Intelligence
- Programmatic Advisory:
  - Identity and Access Management
  - Threat Intelligence Program Maturity
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI)

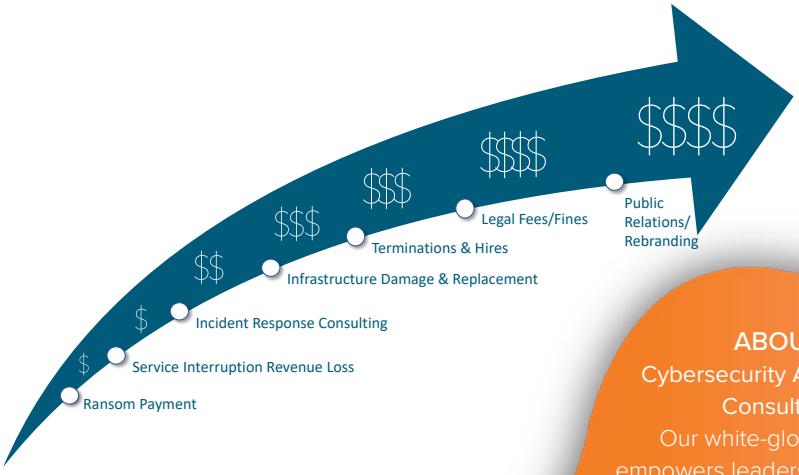
## Companies Impacted by the 'Oktapus' Supply Chain Attack:

The following organizations are a sampling of the over 160 companies targeted in the Oktapus Campaign:

- Twilio
- MailChimp
- Cloudflare
- DoorDash
- Signal
- Telegram
- Klaviyo
- DigitalOcean

## Why Ransomware Matters: Colonial Pipeline Ransomware Attack Cost

The true cost of a ransomware attack expands beyond the ransom.




**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.