TRUEFORT

ARTICLE

How to defend against human operated ransomware

SECURITY

Raj Bhowmick

Raj Bhowmick is Director of Solutions Engineering at TrueFort, where he helps large enterprises protect their application ecosystems from advanced cyber attacks and insider threats.

According to Cybersecurity Ventures, the costs of global ransomware campaigns are expected to increase from $11.5 Billion in 2019 to $20 Billion in 2021.

The same report states companies fell victim to ransomware attacks every 14 seconds in 2019 and predicts it will reach every 11 seconds in 2021.

Ransomware can be delivered via several mechanisms, the most popular of which is often phishing. However, a new category called "Human-Operated" Ransomware is now being used to execute multi-level attacks against company networks.

Here's how it works:

- **Attackers gain initial access to a company's network via a remote desktop protocol (RDP) or phishing attack, and distribute malware like Dridex and Trickbot**
- **They steal user credentials with tools such as Mimikatz and Lazagne**
- **Next they use PowerShell Empire and Cobalt Strike to perform reconnaissance and move laterally across the environment**
- **Finally they use privilege escalation via Domain Administrator access to install ransomware software**

Microsoft has observed that some attackers persist in a victim's environment for months while performing reconnaissance to find crown jewel targets, before dropping ransomware. They often use the victim's infrastructure for bitcoin mining, running SPAM campaigns, and other criminal for profit activities. Adversaries also persist their access so that even after the ransom is paid, they can return for repeat attacks.

Clearly, since ransomware attacks have increased 40% year over year, traditional protection approaches are not working. This is primarily because they focus on the infrastructure layer of IT environments and miss a host of application vulnerabilities. A new approach to enterprise security is gaining popularity, which aims to provide visibility into applications — including their behavior and dependencies — not just network activity.

By monitoring the run-time execution of applications based on processes, identities, and network connections, organizations can establish a baseline for expected behaviors and detect anomalies indicative of ransomware, or other attacks.

This baseline and ongoing visibility enables organizations to identify where application risks reside, including:

- **Exposed internet-facing services such as RDP**
- **Execution of services like RDP and SSH and where they can be used for lateral movement**
- **Out-of-support operating systems, application runtimes like JVMs, and their relationships to sensitive applications that can be exploited by attackers to escalate privileges and move laterally**
- **Privileged credentials that can be used for lateral movement as well as activation of ransomware**

This combination of the application inventory and risk posture visibility can help organizations address risks via fixes, policies and controls. While fixes can address some risks, policies and controls are needed to ensure business critical applications are protected.

These can be implemented in a variety of ways to remediate risks and vulnerabilities that attackers can exploit, such as:

- **Implementing CIS Security and NIST guidelines to automate and enforce industry-standard best practices for server hardening**
- **Using machine learning to automate acceptable use policy generation for allow listing, identity, and network activities in application environments**
- **Enforcing micro-segmentation policies from the endpoint, preventing lateral movement**
- **Performing system integrity monitoring of processes and files to identify unauthorized changes, process injection, and process-hollowing**
- **Implementing behavioral analysis and anomaly detection capabilities for process execution, service account usage and network connections to detect anomalous activity that may be malicious in nature**

In addition, organizations require alerting capabilities to be notified of anomalous events and initiate automated responses such as blocking connections, killing processes, and terminating sessions. Forensics down to process execution trees should accompany alerting to provide indicator of compromise data to help incident response teams reduce identification and containment times.

Unlike traditional malware threats, ransomware attacks can now involve a sophisticated, multi-stage campaign that can last weeks, if not months after attackers gain an initial foothold in the environment. By supplementing infrastructure security monitoring and controls with application-centric security capabilities, organizations can detect ransomware activity early in the kill chain to block and prevent an enterprise-scale compromise.

By supplementing infrastructure security monitoring and controls with application-centric security capabilities, organizations can detect ransomware activity early in the kill chain to block and prevent an enterprise-scale compromise.

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application-centric Fortress platform delivers comprehensive realtime cloud-to-the-ground insight, protection and automated response with patented machine intelligence and a single or bring-your-own agent. Fortress overcomes the application security blindspots inherent in legacy infrastructure-centric tools, providing unparalleled visibility and protection for applications in on-prem, hybrid and cloud environments and for security teams across the enterprise. Fortress speeds response times, minimizes the blast radius of compromises, prioritizes resources, and enhances application risk posture.

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM