Threats and Risks related to Ransomware

Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key. Ransomware can target any PC, MAC or Mobile systems, whether it's a home computer, endpoints in an enterprise network, or servers used by a government agency or healthcare provider. There is no guarantee that paying the ransom will give access to your data again. Law enforcement agencies, CERTs worldwide and FBI highly recommend to not pay the ransom to the adversaries as decryption is by no means guaranteed and paying up actually encourages more Ransomware attacks and threats. In 2016 the world has seen Ransomware used as part of APT attacks on Critical Infrastructure in Israel as well as many other countries and organizations. Most common attack vectors to deploy Ransomware are email attachments and drive-by downloads from infected websites. More sophisticated methods include targeted phishing, social engineering and direct hacking of remote access systems such as VPN, SSH and RDP to use the compromised system as an entry point to deploy Ransomware at server segments or use central servers such as MS Active Directory to infect domain workstations. According to our own research and based on manual review of more than 50 reverse-engineering reports of most common Ransomware malware samples by companies like Symantec, Trend Micro, Kaspersky, Intel Security, ESET and others, more than 50% of Ransomware is using Tor network as part of various attack stages, include C2 and Actions on Objectives. More than 70% of Ransomware can potentially use Tor, so tracking any Tor communications in the organization is important.

Ransomware Hunter is a specialized add-on solution that natively integrates with HPE ArcSight and leverages Stastical Profiling and Behavioral analysis methods, OSINT feeds including Ransomware Tracker by Abuse.ch and SOC Prime's Detect Tor private threat intelligence feed as well as strictly defined correlation rules. With this Use Case organizations are able to spot and stop any Ransomware as early as possible which enables timely Incident Response, Mitigation and prevents further damage, including critical and workstations system downtime, data loss, financial and brand reputation damages.

Best practices to counter Ransomware that may be included in organization security policy

Active Mitigation solutions

1. All internet access needs to be protected with proper mitigation technologies including Email Security Gateways, Web Security Gateways (proxies), EndPoint protection systems etc. All signatures must be kept up to date. This will mitigate and may prevent Ransomware infection at Delivery phase of Cyber Kill Chain.
2. Vulnerability and Patch management programs should be implemented and operated on continuous basis to prevent Ransomware infection at Exploitation Phase. Outdated and non-licensed software should not be used as it is more exposed to Exploitation.
3. Application Whitelisting can prevent Ransomware at Installation phase.

Proactive detection solutions

Since it is not feasible to implement requirements 1-3 for Active Mitigation in all environments and due to adversaries continuously bypassing traditional defense systems in both wide-spectre and targeted attacks, accurate and timely detection followed by Incident Response can completely prevent any threat and damage posed by Ransomware. A SIEM technology combined with Ransomware Hunter Use Case can provide detection and automatic alerting capabilities at Reconnaissance, Delivery, Exploitation, Installation, Command and Control (C2) and Action on Objectives phases, thus covering full threat Life-cycle according to Cyber Kill Chain methodology.

Preventive Measures

1. Security Awareness training is mandatory for any company employees that have access to IT systems, including BYOD and mobile devices. It may be just the factor that prevents a trained employee from opening a malicious email attachment or visiting malicious websites.
2. Regular backups need to be maintained and regularly tested. Backup test results need to be approved by security or internal audit units. Having a secure backup can be exactly what makes a difference between a basic system restore procedure and financial, data and productivity losses.

The information contained herein is result of open source and private research conducted by SOC Prime Inc.
Information is shared on "AS-IS" basis with members of HPE Protect724 community for educational and internal usage.
SOC Prime and SOC Prime logo is trademark of SOC Prime Inc., all other names and trademarks are property of their respective owners.
For any questions and suggestions please contact ucl@socprime.com