Prevenire in modalità proattiva un attacco ramsomware in ambienti IT, AD e OT

Paolo Florian
Sales Engineer
pflorian@tenable.com
Unparalleled visibility into the modern attack surface with IT, OT, AD, Cloud and Web-App sensors.

Prioritize remediation effort and reduce the probability of a business impacting cyber event occurring through the power of prediction.

Be business-aligned by communicating risk and effectiveness in a common language.
94% of organizations have experienced a business impacting cyber attack or compromise in the last 12 months.

RYUK leverages CVE-2020-1472 to move from initial phish to domain admin in 5 hours.

16.2 days on average to recover from a ransomware attack.

Average Global Ransomware Demand

<table>
<thead>
<tr>
<th>Year</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$4,300</td>
<td>$5,900</td>
<td>$5,600</td>
</tr>
</tbody>
</table>

Average downtime cost as a result

<table>
<thead>
<tr>
<th>Year</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$46,800</td>
<td>$141,000</td>
<td>$274,200</td>
</tr>
</tbody>
</table>
**Initial Foothold**

via phishing or vulnerability

<table>
<thead>
<tr>
<th>DISRUPT ATTACK PATHS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explore</strong></td>
</tr>
<tr>
<td><strong>Elevate</strong></td>
</tr>
<tr>
<td><strong>Evade</strong></td>
</tr>
<tr>
<td><strong>Establish</strong></td>
</tr>
<tr>
<td><strong>Exfiltrate</strong></td>
</tr>
</tbody>
</table>

---

Know the misconfigurations and vulnerabilities used to elevate permissions within Active Directory

Identify indicators of privilege escalation and lateral movement
1. Scan Often – Scan Everything

Ransomware strains are using software vulnerabilities as the initial attack vector. These tend to be older and well known, so it’s essential to continuously assess your entire attack surface.
RANSOMWARE ATTACKS, ALL CONCERNED – HOW TO PREVENT THEM AND RESPOND TO AN INCIDENT

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
- Regularly patch and update software and OSs to the latest available versions.
- Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.

https://www.ssi.gouv.fr/en/guide/ransomware-attacks-all-concerned/
Look for Old Vulnerabilities, Find Those Likely To Be Exploited & Patch.... Patch... Patch...

February 11, 2021

Researchers identify 223 vulnerabilities used in recent ransomware attacks

The vast majority of flaws (96%) used in ransomware attacks are years old, having been publicly identified prior to 2019. The oldest, CVE-2007-1036, is a remote code execution vulnerability first discovered back in 2007, which researchers continue to see exploited in the wild.
Major Cyber Attacks on OT Infrastructures
A Historical Timeline

- **Stuxnet Aurora** (2010)
- **Night Dragon** (2011)
- **Shamoon Dragonfly** (2012)
- **Red October** (2013)
- **Havex Steel Mill Attack** (2014)
- **Op Ghoul** (2016)
- **Wannacry** and **Triton** (2017)
- **Petya** (2018)
- **Shamoon3 VPNFilter Alert (TA18-074A)** (2019)
- **LockerGoga Dtrack Lemon Duck** (2020)
- **Solarwinds FL Water Colonial JBS** (2021)
2. Harden AD – Protect Crown Jewels

Ransomware groups have ditched their custom spreader code used to propagate attacks in favor of a more effective technology already present in organizations: Active Directory.
SECURE YOUR ACTIVE DIRECTORY AND DISRUPT ATTACK PATHS

1. FIND AND FIX YOUR EXISTING WEAKNESSES
   - Immediately discover, map, and score existing weaknesses
   - Follow step-by-step remediation tactics and prevent attacks

2. UNCOVER NEW ATTACK PATHS
   - Continuously identify new vulnerabilities and misconfigurations
   - Break attack pathways and keep your threat exposure in check

3. DETECT ONGOING ATTACKS IN REAL TIME
   - Get alerts and actionable remediation plans on AD attacks
   - Enrich your SIEM with ongoing attack information

4. INVESTIGATE INCIDENTS AND HUNT FOR THREATS
   - Search and correlate AD changes at object and attribute levels
   - Trigger response playbooks in your SOAR
3. De-Escalate Privilege Escalation

Monitor AD for unusual activity. AD changes, Syslog changes and Windows event logs can be correlated to reveal misuses of privileged accounts and active misconfiguration exploits.
Discover the underlying issues affecting your Active Directory
- Identify dangerous trust relationships
- Catch every change in your AD
- Make the link between AD changes and malicious actions
- Analyze in-depth details of attacks
- Explore MITRE ATT&CK descriptions directly from incident detail

NO AGENTS

NO PRIVILEGES

AD-NATIVE

NEAR-INSTANT VALUE
4. Prioritize Using Prediction

Fix first what matters most. Take advantage of real-time threat intelligence to know which vulns are being attacked. In addition, vulnerabilities targeted by ransomware cluster around specific types of weaknesses and asset categories. Prioritize and proactively address these specific vulnerabilities first.
Needles In The Haystack
The Vast Majority Of Vulns Pose Little To No Risk

5.2% have exploits published

Few vulnerabilities are ever exploited in the wild

Source: Tenable Research
Leverages supervised machine learning algorithms to calculate the priority of a vulnerability based on the real threat posed. Key Drivers include:

- Threat Recency
- Threat Intensity
- Exploitability
- Vulnerability Age
- Threat Sources
5. Remediate Like Your Org Depends On It

Vulnerabilities targeted for remediation are often never fully remediated. Integrate risk-based vulnerability management solutions integrate with your ITSM and ticketing systems to automate workflows, correlate vulnerabilities with patches, and verify that all instances of a vulnerability have been patched or remediated by a compensating control.
6. Improve Your Game – Measure

Develop key metrics to measure and communicate how operational controls are working (or not). Benchmark data to compare performance across internal groups and externally against your peers. Measure cyber hygiene practices such as assessment capabilities, remediation speed and overall cyber risk reduction.
MEASURE EFFECTIVENESS & EXPOSURE TO IMPROVE

<table>
<thead>
<tr>
<th>Assessment Maturity</th>
<th>Remediation Maturity</th>
<th>Mitigations</th>
<th>Cyber Exposure Score</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure and compare how effectively the security team identifies assets and vulnerabilities</td>
<td>Measure and compare how effectively the operations team address critical issues</td>
<td>Ensure third party endpoint controls are deployed and configured to mitigate flaws</td>
<td>An objective score of the organization, business unit or assets cyber risk</td>
<td>Drive improvement at the business process level to increase visibility and reduce cyber risk</td>
</tr>
</tbody>
</table>
GREAT SECURITY STARTS WITH COMPLETE AND CONTINUOUS VISIBILITY OF YOUR MODERN ATTACK SURFACE
Questions

pflorian@tenable.com