Ransomware Outfits Announcing Support for Russia in the Event of Cyber Attacks

Executive Summary
This is an Optiv Global Threat Intelligence Center (gTIC) Notification Advisory. The purpose of this Notification is for situational awareness related to the cyber security threat landscape, and does not indicate an imminent threat.

As of February 25, 2022, ransomware groups including Conti, RedBandit and CoomingProject announced preparations to attack any country that threatened attacks or sanctions against Russia as part of the ongoing military invasion in Ukraine since February 23. Optiv gTIC is providing this information to Optiv customers for situational awareness, and there is no indication of imminent threat or targeting against any company, vertical, or organization at the time of this report. Optiv gTIC’s assessment of the ransomware threat to organizations across all industries echoes our previous assessment prior to the Russian operation in Ukraine. Ransomware remains one of the most relevant threats to all organizations and is Likely to increase over the next 12 months, an assessment the gTIC has maintained previously.

Optiv gTIC reiterates that’s organizations in key industry verticals likes Energy, Utilities, Transportation, Telecommunications, Government, and Financials remain at higher risk of disruptive cyber campaigns like ransomware, Denial-of-Service (DoS), and destructive wiper malware. Organizations are encouraged to follow previously established defense-in-depth policies and mitigations recommended for ransomware activity regardless of attribution and threat level. Optiv’s gTIC will continue to monitor the cyber-threat landscape situation as a result of Russian aggression in Ukraine and provide updates where applicable.

Key Findings and Analysis

Key Findings
• On February 25, 2022, the Conti Ransomware group announced its allegiance to Russia and threatened to attack “critical infrastructures of an enemy” (NFI) on its data leak page.
Lesser known and lower-capable ransomware outfits like CoomingProject and RedBandit also released messages threatening counterattacks against organizations and countries that carry out any attacks against Russia.

Optiv gTIC Analysis and Comments
Optiv gTIC assess with High Confidence that “critical infrastructures” referenced in the Conti Ransomware threat is not strictly limited to traditional critical infrastructure companies like Utilities and Energy and industrial control systems/supervisory control and data acquisition (ICS/SCADA), but will also include organizations in other key verticals including Financials, Transportation, Telecommunications, and Government.

There is currently no information or evidence of an imminent threat against organizations in any particular vertical or country. Ransomware attacks will Likely increase over the next 12 months, and is an estimate that Optiv gTIC has maintained prior to the recent military actions in Ukraine. The over ransomware threat landscape is not changed by these recent messages, and organizations are encouraged to follow long-standing mitigation and defense-in-depth measure previously recommended.

Tools and techniques leveraged by Conti and other ransomware outfits, as observed by Optiv gTIC over the last 12 months, include leveraging vulnerabilities in widely used and ubiquitous software and open-source and commercial IT management and administrator tools. These same techniques, tools, and procedures will Very Likely be used over the next 12 months. The following is a list of these tools, techniques, and procedures leveraged by the Conti Ransomware outfit:

- Open-source and IT/Administrator Tools:
- AnyDesk (Persistance, Discovery, Defense Evasion)
- Rclone (Discovery)
- MEGA file transfer service (Exfiltration)
- Ngrok reverse proxy (Exfiltration, Command-and-Control)
- AdFind (Discovery, Credential Access, Collection)
- PsExec (Execution, Privilege Escalation, Discovery, Lateral Movement, Collection)
- PC Hunter (Discovery)

Techniques and Software and Services Exploited

- RDP (Initial Access)
- Phishing (Initial Access, Execution)
- Log4j CVE-2021-44228 “Log4Shell” (Initial Access, Privilege Escalation)
- MS Exchange CVE-2021-31207/34473/34523 “ProxyLogon” (Initial Access, Collection)
- MS NetLogon CVE-2020-1472 “ZeroLogon” (Privilege Escalation, Exfiltration, Credential Access, Discovery)
- MS Print Spooler CVE-2021-1675 (Privilege Escalation, Execution)
- Process: net.exe stop * /y (Defense Evasion)
- Process: wmic.exe shadowcopy * delete (Impact)

Mitigation Recommendations

Optiv’s gTIC makes the following recommendations on mitigation for the threats highlighted in this report:

- Ensure that all remote access to organizations’ network and administrative access requires multi-factor authentication (MFA) and users account activities are dictated by least-privilege policies.
- Ensure that a vulnerability management program is in place that prioritizes patching based on the severity of a vulnerability, the number of systems and devices affected, and how widely known the vulnerability is.
- Ensure all ports and protocols that are not essential are disabled and not Internet-facing. These include Remote Desktop Protocol (RDP) and Universal Plug-and-Play (UPnP)
- Deploy endpoint security controls to monitor for behavioral indicators of compromise and deny unwanted code execution
- Employ behavior-based detection and preventive measures, rather than attribution-based indicators.
- Ensure that all vendors and partners in the supply chain are held to the same security standards and affected organizations’ traffic is isolated and closely reviewed.
- Create and implement an incident response plan that includes a designated incident response team.
• Conduct penetration testing to identify points of weakness; combine with tabletop exercises to ensure the incident response plan is effective and all members of the incident response team understand their roles in the event of a cyber-attack.

• Ensure offline backups are available, they are updated, and they can effectively be used in the event of an incident.
Appendix A – References

Vail, Emma (2022, February 25) Russia or Ukraine: Hacking Groups Take Sides. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
Appendix B – Assessments and Probability Statements

Analytical Comments and Probability Statements

**Most Likely Course of Action (MLCOA)** – the expected and probable tactics, techniques, and actions carried out by a threat actor. COA statements are well established and accepted in estimative and predictive intelligence assessments.

**Most Dangerous Course of Action (MDCOA)** – tactics, techniques, or actions carried out or taken by an adversary that result in a worst-case scenario outcome or impact, regardless of probability. COA statements are well established and accepted in estimative and predictive intelligence assessments.

**Words of Estimated Probability** – Optiv EIM Intelligence employs the use of both probability statements for likelihood of events or actions and confidence levels for analytic assessments and judgements. Probability statements and confidence statements are inherently subjective; however, Optiv EIM Intelligence leverages professional experience and intelligence fundamentals to deliver reasonable and relevant statements and assessments. Probability statements and the degree of likelihood of an assessed event/incident are modeled after the *Intelligence Community Directive (ICD) 203: Analytic Standards*, published by the United States’ Office of the Director of National Intelligence (ODNI), and are as follows:

<table>
<thead>
<tr>
<th>Confidence Level</th>
<th>Optiv EIM Definition</th>
<th>Factors</th>
<th>Quantitative Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Confidence</td>
<td>information and/or intelligence is assessed to be of high reliability and value to drive operations and decision</td>
<td>Established history, repeated observations and patterns, strong precedence to form professional assessment and prediction/extrapolation</td>
<td>75%+</td>
</tr>
<tr>
<td>Moderate Confidence</td>
<td>information and/or intelligence is reasonable and warrants consideration or action or response where applicable</td>
<td>Sporadic observations, limited historical references (too recent or too long of a gap to be considered &quot;established&quot;)</td>
<td>45-65% (+/- 10%)</td>
</tr>
<tr>
<td>Low Confidence</td>
<td>Information and/or intelligence is unreliable or less relevant and provided as situational awareness</td>
<td>lack of established history or observations, unreliable or circumstantial evidence</td>
<td>&lt; 35%</td>
</tr>
</tbody>
</table>

Per *ICD 203* standards, confidence-level statements are not combined with probability and degree of likelihood terms proposed in the above chart.