Jefferson Wells™
ManpowerGroup

Emerging Insight…
The Ransomware Epidemic

Ransomware has become a critical cyber threat to businesses in all industries over the past two years. Fueled by the near complete anonymity and the limited capability of law enforcement to trace and recover cryptocurrency transactions, cyber criminals have become emboldened to attack any targets they believe can be successfully compromised and coerced into paying a ransom. Yet despite the increased frequency of attacks and the catastrophic impacts to organizations, ransomware is attributed to only 10% (ranked third most common) of all attacks within today's business environment.

Who are the perpetrators of ransomware attacks?

The ransomware epidemic began in 2016, when the authors of ransomware determined they could make a lot more money, and at much lower risk, if they offered to sell or rent their tools – Ransomware-as-a-Services was born. This form of attack is becoming more predominant as results are very lucrative for the 'service providers' behind the tools.

Breaking Down Ransomware Attack Personas

Threat Actors	Motives	Attack Targets	Risks
Nation State	• Political Agenda • Military Agenda • Economic Harm	• Critical Infrastructure • Intellectual Property • Business Systems	• Business Disruption • Data Disclosure • Political Impacts
Criminal Underground	• Financial Gain • Political Benefit • Social Impact	• Sensitive Information • Business Systems • Critical Infrastructure	• Business Disruption • Financial Impact • Information Loss
Hacktivists	• *Political Agenda* • *Personal Agenda* • *Social Change*	• *Corporate Data* • *Employee Information*	• *Brand Damage* • *Business Disruption* • *Loss of Reputation*
Lone Wolves	• *Thrill Seeking* • *Personal Gain* • *Social Status*	• *Device Control* • *Vandalism* • *Harassment*	• *Business Disruption* • *Brand Damage* • *Personal Safety*
Insiders	• *Financial Gain* • *Social/Political Gain* • *Revenge*	• *Device Control* • *Vandalism* • *Harassment*	• *Competitive Impact* • *Business Disruption* • *Loss of Reputation*

How does a ransomware attack work?

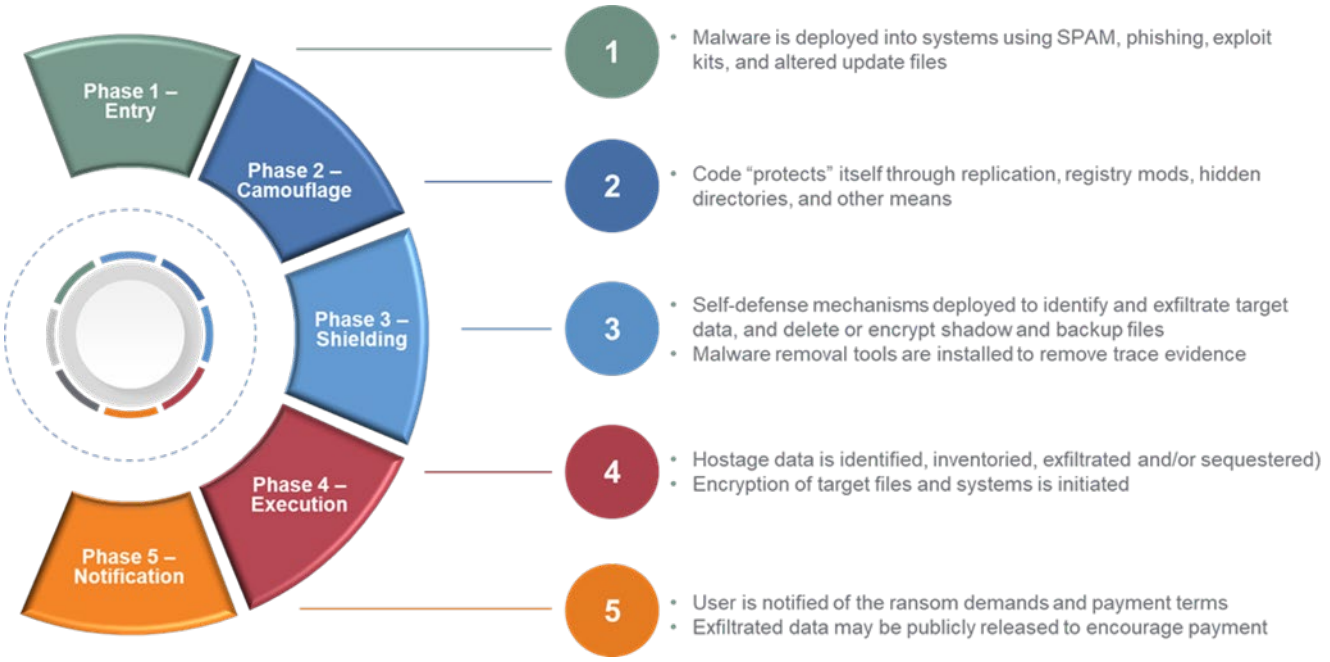
Ransomware attacks are malware-based attacks crafted to encrypt data on computer systems located in the target organization. Most of these attacks begin with some form of phishing, enabled via SPAM email with malicious attachments or links to compromised websites.

Once an initial user or system is compromised, the attack progresses with the goal of deploying a payload capable of completing the remaining phases of the attack, including the on-command exfiltration and encryption of discovered data.

Key Defensive Measures

- Keep systems maintained
  - Perform vulnerability scans and pen tests
  - Deploy patches quickly and comprehensively
- Limit your attack surface
  - Restrict ports/protocols
  - Limit access rights
  - Minimize mount points
- Train your personnel
  - Awareness training
  - Phishing tests
  - Incident response
- Reduce your exposure
  - Email filters
  - Browser filters
  - Software whitelists

Anatomy of a Ransomware Attack



Recent evolution of ransomware attacks threatens the public release of captured data to entice the victim to reconsider any temptation to refuse to pay the ransom. This technique has been particularly useful when the attacker believes the victim will find it cost effective to pay rather than risk public humiliation. It is clear from the new attack components that ransomware attackers are executing a playbook based on using whatever techniques are needed to generate revenue. As ransomware is now a business, the attack techniques are expected to continue to evolve as defensive measures begin to reduce the effectiveness of ransomware attacks.

What are some common flaws that enable ransomware?

Analysis of publicly disclosed ransomware attacks has revealed several flaws that were either already known by the victims or should have been discovered by typical governance and oversight processes recommended by security and IT professionals. In many cases,

- Internet-facing systems had vulnerabilities that were not patched
- Employees were somewhat or highly susceptible to phishing attacks, and
- Data backup programs were either nonexistent or had not been fully tested in a long while.

Each of these flaws enabled the ransomware attackers to enter the enterprise and launch the malware. Even though each of these flows had well-known methods and tools to reduce their ability to be exploited, the victim organizations failed to prioritize and fund these activities.

In addition, victims also tended to have one or more of the common process and control flaws, such as:

Privileges exceeded those required for assigned duties

- Organizations often opt for user convenience over user awareness
- Network and system access often lacks basic segmentation rules

Attackers rely on excess privileges to extend attack

Core repositories allowed bulk access and/or transfer

- Rules did not limit users' ability to view/retrieve sensitive data sets
- Many instances of full aggregation of sensitive data in a single repository

Write privileges are routinely given whether needed or not

Core systems had weak controls and monitoring

- Monitoring, reporting and audits missed critical weaknesses
- Many "victims" failed to use strong authentication methods for core data

Many ransomware attacks are largely preventable

Ransomware Response 101

Establishing an effective response capability to deal with ransomware involves three primary focus areas: **Detection, Isolation,** and **Data Protection.** The most important of these is the detection capability, which must have the sensors, analytics, and triggering capabilities needed to initiate the incident response team. The response actions then move to the isolation of infected (or suspected) systems, networks, and applications to reduce the ability of the malware to spread further. The final capability area is determining backup and recovery copies of critical data and the system configuration files needed to restore services.

Detection

- Utilize automatic alerting of potential/actual ransomware attacks
- Monitor, trigger, and respond to filters and logs (including anti-virus, anti-malware, network, application, and data transfer logs

Isolation

- Isolate infected systems, applications, and data repositories
- Disconnect and quarantine primary assets, including wireless connectivity
- Disconnect and quarantine interconnected secondary assets required for recovery

Data Protection

- Isolate on-line repositories, backups, and recovery sources
- Evaluate and quarantine live and shadow copies of data
- Identify and retrieve “Gold Masters” needed to support

Preparations that significantly reduce your risk

Various preparations are available to reduce your exposure and risk from ransomware and other forms of malware-based attacks. Many of these precautions are also beneficial in improving your organization’s operational efficiency, security, and stability.

People

Awareness

- Establish initial and periodic training on threats, risks, user responsibilities, and processes
- Make security training a business requirement and integrate into compensation where possible
- Ensure constant testing of knowledge and institutional cyber risk ‘muscle-memory’
- Deliver regular executive briefings and workshops (C-Suite, Board, Audit Committee)
- Publish and report key meaningful management metrics for cyber risk and risk posture

Planning

- Pragmatic, holistic, and inclusive risk-based strategic cyber resilience plan
- Periodic business resilience planning, review and revision that includes ransomware
- Scenario-based strategies and plans for key cyber risks
- Cyber risk 1-year, 3-year, 5-year investment plans with quarterly reviews
- Customer and supply chain engagement, awareness, response, and communication plans

Networks

Limit Exposure

- Multi-tier network architecture to segment core business systems
- Multi-tier application architecture to ensure protocol isolation
- NAC and MFA for all networks hosting sensitive data, applications, systems, repositories
- Restrictions on outbound ad-hoc internal/Internet connections from critical networks

Limit Spread

- Advanced filtering gateways for email, web, application connectivity,
- Micro-segmentation to limit direct connectivity to/from critical networks/hosts/apps,
- Virtual or actual air-gapping of backup systems/mechanisms,
- Protocol filtering to reduce internetwork persistent server mounting

Operational Technology and Industrial Control Systems

For organizations that are part of the National Critical Infrastructure or have OT (Operational Technology), ICS (Industrial Control System), and/or SCADA (Supervisory Control And Data Acquisition) networks, additional considerations are warranted:

- Air gap OT, ICS, and SCADA networks wherever feasible
- Minimize the connection points where connectivity is required
- Block ALL Internet and external access to/from the networks
- Disable all in-bound initiated communications to the networks
- Utilize VPNs, VDI hosts and MFA for all access directly to systems
- Establish strict filtering and firewall controls for all communications
- Ensure all connectivity uses encrypted private networks or tunnels
- Organize and isolate resources into logical and physical zones
- Restrict the use of business applications on OT, ICS, and SCADA systems

Business Operational

Some victims of ransomware shut down their primary Operational Technology (OT) and Industrial Control Systems (ICS) during response activities; not because they were impacted by the ransomware, but, because the business systems needed to provide inventory management, logistics, and billing related to the output of the OT or ICS systems were compromised. To avoid this type of impact, there are times when business operational networks should be treated like OT and ICS networks with additional technical controls and processes limiting the susceptibility of critical business systems to malware attacks. The following are a few of the questions that might lead you to reclassify a business network as a Business Operational Network and implement additional controls and monitoring:

- **Who is on the network?** Is there a reason justifying each of the users attached to the network?
- **What is on the network?** Is every resource on the network key to your business revenue?
- **When is it connected?** Are any file shares on the network required to be persistent?
- **Where is it connected?** Is the connectivity to/from the network required or just convenient?
- **Why is it here?** Is each service, application and/or repository on the network required?

The bottom line: determining you have implemented an appropriate level of isolation, segmentation, and technical control based on the criticality of each network, system, and application to your business.

Response

Roles, Skills, and Resourcing

- Develop and maintain a comprehensive matrix of resources – internal and third-party
- Identify at least a secondary resource for all critical response roles
- Do the same for all key business leadership and corporate support roles
- Include essential law enforcement and national/regional government liaison roles
- Establish a contact list that is managed and disseminated real time to resources

Response – Readiness Evaluation

- Execute periodic readiness tests (tabletop and live) for all scenarios
- Ensure random response resources are ‘unavailable’
- Include law enforcement and government liaison participation whenever possible
- Enlist audit group or third party to oversee and evaluate response tests periodically

Key Preparation Elements

In addition to the identified preparations above, it is also worth reviewing your organization’s preparation and response planning to be sure the following key preparation elements have not been overlooked:

- **Asset Management** – organizations often lack complete information on how many devices they have, where they reside on the network, what O/S each is running, etc.
- **Controls Management** – many organizations have inadequate monitoring of controls, which limits their ability to determine how well they are protected
- **Configuration and Change Management** – too often organizations focus on getting applications deployed and then fail to follow through on properly maintaining them

- **Vulnerability Management** – most ransomware victims had a critical system with a known but unpatched vulnerability which became the entry point for the attack
- **Incident Management** – organizations often lack sufficient integration and coordination of technical response teams and the business crisis management team
- **Audit** – many organizations focus on evaluating controls and fail to adequately deploy the governance and oversight processes that dramatically reduce the risk of ransomware

All organizations should understand and accept two things - ransomware is here to stay, and it will continue to evolve, which means the height of the bar for determining adequate security will also continue to rise. In response, every organization should regularly review their current cyber risk profile and then take appropriate steps to improve their ability to detect, defend, and respond to ransomware. But the call to action does not end there. Every organization also needs to recognize that ransomware is only one of the top forms of cyber-attack, so additional consideration must also be given to strengthening cyber defenses that reduce the organization's susceptibility to all known forms of cyber risk.

Authored by

Michael Gerdes
Director, Cyber Risk Center of Expertise
585.981.0042
michael.gerdes@jeffersonwells.com

Mike has over 40 years' information security and technology executive management and professional services consulting experience. His global business experience includes leading the security programs at two Fortune 100 companies and over 20 years providing cyber risk, information security, and privacy strategic thought leadership, governance, compliance, risk management and technology solutions for clients in financial services, healthcare, insurance, retail, and other industries.