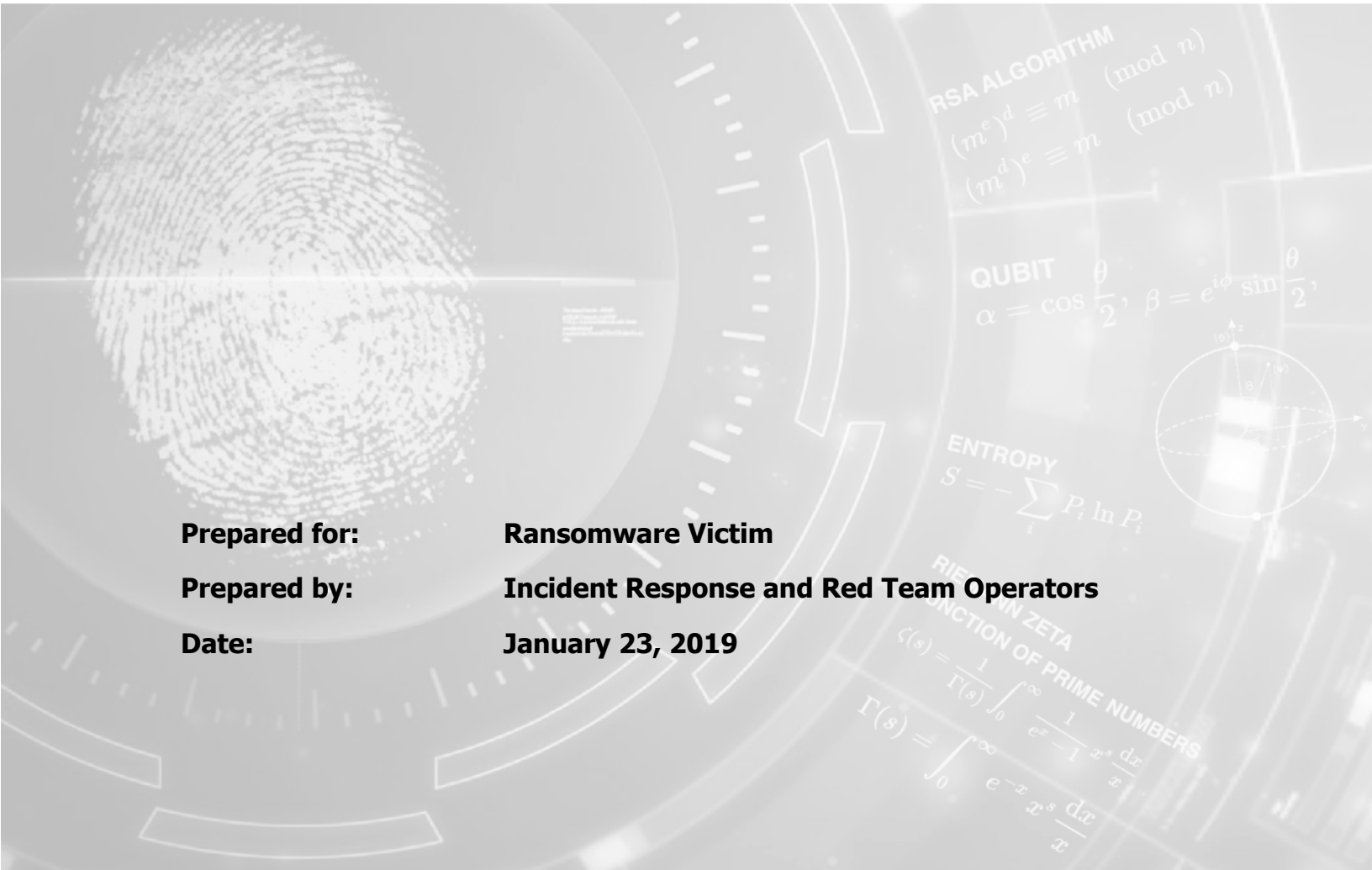
LIFARS
your digital world, **secured**

Ransomware Response Guideline

Digital Forensics and Incident Response Unit



Prepared for: **Ransomware Victim**

Prepared by: **Incident Response and Red Team Operators**

Date: **January 23, 2019**

Ransomware Definition

Like the name implies, ransomware is essentially digital extortion that is executed through software that uses encryption techniques to keep files and entire systems locked from use by their original owner and holds them hostage until (theoretically) a payment has been made.

Once ransomware enters a system, it makes itself known by taking control, encrypting files or complete systems, and blocking user access until requests for payments, which are often displayed in warning messages, are fulfilled. Unfortunately, there is no guarantee that the keys needed to break the encryption will be returned upon payment.

This devious malware typically enters opportunistically through drive-by downloads, email links, social network messages, and websites; more recently, ransomware has been distributed through aggressive worms and targeted attacks. Ransomware, like many Trojans, are disguised as legitimate files, with the ransom note appearing on screen, often with threats of deletion or publication without payment. The result is often brand damage, costly lawsuits, or lost customer loyalty.

Attacks such as WannaCry, Petya, Bad Rabbit were headliners in 2017 and 2018. WannaCry alone spread globally to 300,000 devices in over 150 countries in a single weekend, and caused millions, perhaps even billions, of damage.

Ransomware Containment and Remediation

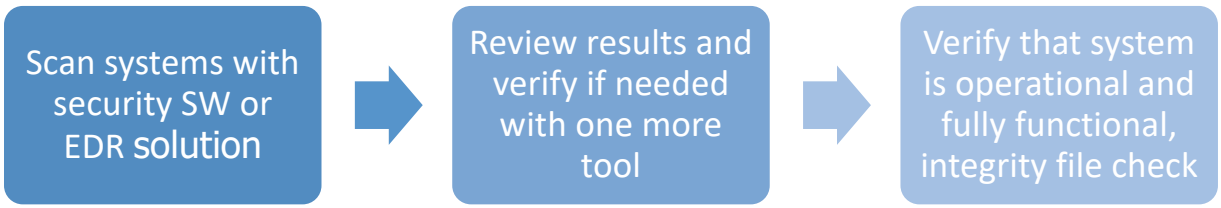
Detection

Ransomware detection can be done various ways and possible scenarios are:

- Endpoint security software detection – can be antivirus, or stronger EDR solution
- Threat intelligence detection – deploying solutions that can scan systems and networks for Indicators of Compromise (IoCs), DNS protecting solutions such as OpenDNS and similar, lateral movement behavior in data flow
- SIEM or log reviews – often execution of ransomware is detected from log analysis process
- Network detection sensors – IDS/IPS, UTM firewalls, or other network devices can have tools and sensors that can detect propagation and lateral movement of ransomware, Artificial Intelligence tools such as Darktrace
- Threat Hunting – mostly leveraged by larger organizations and focused on forensic analysis of various artifacts
- Digital forensic investigation and Incident Response – if suspected, forensic analysis can reveal potential compromise

Containment

One of the biggest reasons why malware is so harmful is that it can spread throughout a network very quickly, effecting as much damage in as little time as possible. The goal of any good ransomware response strategy should be to isolate and contain the virus before it has a chance to proliferate. This can dramatically reduce the potential damage the virus can inflict.



Containment customer specific steps:

Endpoint Security Software

- Client should use Windows Defender, and Malware Bytes and scan every endpoint
- Every system should be scanned and if malware is found, report to LIFARS

System verification

- Damaged systems should be reinstalled, or repaired by system instalations files
- Systems that reached life and technology limits, should be replaced

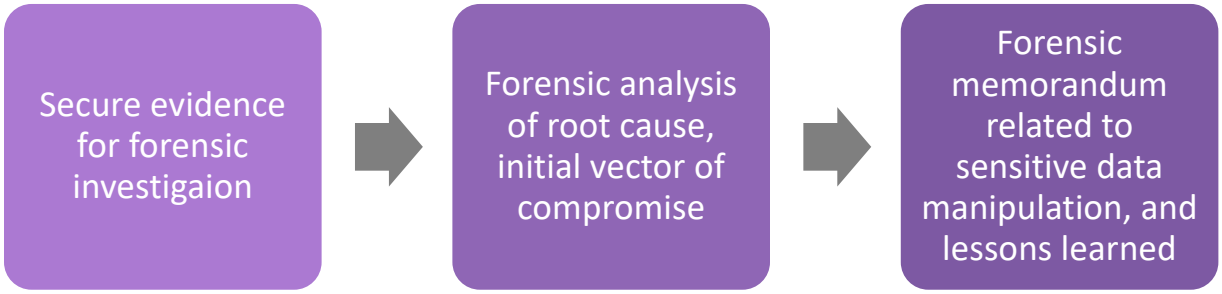
Eradicate

Once the ransomware virus is detected and contained, the next step is to eradicate it from the network. Any machines affected should either be replaced or thoroughly cleaned and continuously monitored thereafter.

Ensure system is clean and functional → System restore, backup restore, repair damages, resintall OS if needed → Verify operational systems, and if needed, replace dameged systems

Recover

As mentioned above, it's critical to regularly back up your files. Once you've done so, deleting the infected files and restoring the good ones is easy. Your data remains safe and the criminals leave empty handed. As part of the recovery process, an forensic investigation should be conducted to further identify sources of potential vulnerabilities as well as processes and policies that may need revision in order to prevent future attacks.



Business can recover well if technological maturity meats with needed level of cyber security posture. Without fully operational technological skeleton, cyber security strategies do not have strong pillars to based its foundation and reinforce protection for the environment.

Ransomware Prevention and Reduction Strategies

Backups: The only options for recovering data after a ransomware infection are to restore it from backup files, or to pay the ransom. However, paying the ransom is no guarantee that the malware will be eradicated, or that it won't return. Further, it is not possible to decrypt without the keys, and it is extremely unlikely to recover the keys via law enforcement action including the FBI.

Disaster Recovery: Organizations must have effective and tested disaster recovery plans with verified off-line backups. Our team has seen several new variants in the wild that target and destroy an organization's backup infrastructure – including Commvault, TSM and most others.

Have a Plan: Having a plan to detect, respond and contain an incident saves valuable time during an incident. Consider investing in endpoint detection and response tools, as well as log correlation to spot ransomware quickly, help you understand where it is coming from, and assist in containment.

Zero-Day Detection Capabilities: Signature based technologies are not effective in detecting a majority of malware today due to the ease in which a given piece of malware can be camouflaged or "packed" to slip past traditional AV.

1. Ensure your network and endpoint protection have the ability to detect and defend against obfuscated malware or zero-day attacks.
2. Consider implementing network devices that can block by file type and provide application control to the endpoint device.

End User Education: Users are often the weakest link in security infrastructure. We all must educate our end users to be very suspicious of risky messages and services. User education programs provide key training and encourage cautious behaviors. Providing incentives to users for identifying real phishing or malicious emails may be also be helpful.

Close Internet Open Ports: IT administrators, third party vendors Users are often accessing network via third party connections, such TeamViewer, LogMeIn, GoToMyPC, and similar. Access control to third party connectivity has to be strictly enforced and controlled. Remote Desktop Connection (RDP), File Transfer Protocol (FTP), and similar direct access is often used for hacking into the network, especially if credentials are weak, or systems are not patched.

True-up User Access Permissions: Reduce data attack surface exposed to ransomware by strictly governing what users have access to. Administrators should never use their admin accounts for day-to-day business such as email, because mapped drives are an easy and fast

vector for the malware to encrypt file server data. Several excellent tools are available to help organizations quickly detect anomalous user file access and change behavior.

Vulnerability and Patch Management: Regularly conduct internal and external vulnerability scans, then mitigate. Vulnerability and patch management isn't fun for anyone, but it is the foundation of a good security program for all threats – including ransomware.

Block Unnecessary File Types: Tune your mail protection to block unnecessary file types. Block all unnecessary file types over email including ".exe" if possible.

Show Full File Extensions: Ransomware often arrives as .pdf.exe. Enabling visibility of full file extensions makes suspicious files easier to spot.

Alert on Anomalous User Behavior: By setting up notifications to alert you about an abnormal user or system behavior, organizations may detect an outbreak early – when it's easier to contain. Understanding abnormal system or user behavior – particularly file encryption – can tip you off to ransomware and allow you to thwart the attack. User behavior analytics is a powerful tool for many threats including ransomware.

Consider Deploying a Honeypot and Deception Technologies: Deploying a honeypot may slow a ransomware or other attack and can help provide early detection. Ransomware delivers a "help me" file to "assist" the users in paying the ransom. Organizations may allow it to be written and send an email alert to the helpdesk, security team, and server admins that includes the file location and the user account used to write it.

It is also important to remember that in regard to security, no two organizations are exactly alike. Sirius has a dedicated team of security experts that can discuss and develop a customized plan that is specific to your company.

LIFARS
your digital world, **secured**

About Us

LIFARS is the global leader in Incident Response, Digital Forensics, Ransomware mitigation and Cyber Resiliency Services. At LIFARS, we believe that cybersecurity is a matter of trust – that is why most of our services are rendered onsite at your premises to establish a personal relationship. Our solutions are based on industry best practices and hands-on expertise stemming from decades of experience. LIFARS conducts digital forensic investigations, incident response, web application security testing, digital risk assessments and academic research. LIFARS continuously explores the latest innovation in the cybersecurity field and seeks to stay one step ahead of tomorrow's industry landscape.

Cyber experience spans decades working on high profile events often in coordination with Law Enforcement Agencies around the world. Best in class methodology derives directly and indirectly from our experience working with and for US Intelligence Agencies, US Secret Service, FBI, DHS as well as Interpol, Europol and NATO.

Why LIFARS

At LIFARS, we understand how security organizations operate in a detail-oriented, high-tech manner. We investigate and uncover new threats before attackers can exploit them. Every technology has its own limitations. Our humanized approach to cyber defense consists of layers connecting threat intelligence and response. Today's cyber-world is a maze of complexities. Intricate knowledge of laws, compliance, technologies, mobility, social networking, and the behavioral science of human interaction are essential to defend your networks. Our services and solutions address common challenges and weaknesses in today's connected world.

Speed

Time is money. LIFARS gets you back up running swiftly and securely.

Precision

LIFARS collects evidence for prosecution where others have failed.

Expertise

LIFARS has elite knowledge and insight called upon by intelligence and law enforcement agencies.

Industry Recognition

LIFARS is ranked as one of the top Digital Forensics and Cyber Investigations companies in 2016 and as one of the top cybersecurity companies in the New York metropolitan area for 2015 on the Cybersecurity 500 a directory of the hottest and most innovative companies to watch in the cybersecurity industry.

LIFARS' Approach

LIFARS believes that success is achieved by building partnerships with clients, partners, and employees based on dedication, loyalty, and mutual respect. These qualities along with our business practices and the overall effectiveness of our solutions continue to drive our success and establish us as the leading solutions provider in our industry.

Disclaimer

The information provided in this advisory is provided "as is" without warranty of any kind. LIFARS disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall LIFARS or its partners be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages. Content of this report should be redacted before sharing or published.