Mandiant

WHITE PAPER

Determine your Cybersecurity Risk with Repurposed Ransomware

The Serious Threat of Ransomware

Ransomware attacks continue to target organizations across the business spectrum, from healthcare providers and insurance companies to hotel chains, retail brands, industrial giants and utility companies, as well as state and local governments. By examining trends in ransomware targets, it is becoming clear that some threat actors are motivated not just by financial gain, but also by the ability to disrupt networks, challenge the delivery of public safety services, control critical infrastructure, and alter the delivery of life-saving health services. And that's just scratching the surface of the deep damage ransomware attacks can inflict.

Several examples paint a picture of the destructive nature of ransomware attacks.

- An Alabama hospital that experienced a ransomware attack in 2019 is now facing a medical malpractice suit filed by the family of a newborn baby who died while in the hospital's care.[1] The suit alleges that a non-functioning computer system caused the baby's death because doctors and nurses did not have access to medical alarms and alerts.
- The disruption of the Colonial Pipeline--which is the largest fuel pipeline in the US supplying oil to 12 states--was down for several days because of a ransomware attack in late 2021.[2]
- In early 2022, a breach essentially shut down a local county government.[3] Security camera feeds from jails were blocked and automatic lock systems malfunctioned. Government buildings had to close down, and public safety agencies had to operate on backup systems.
- A large microchip producer was attacked by the ransomware gang known as Lapsus$. The group said it would release 1 TB of data—including access credentials, proprietary data and source code—forcing parts of the company to go offline for two days at a huge earnings loss.[4]
- A major sports organization was attacked by the hacker group Babuk, which said it had stolen 500 GB of confidential data, including players' contracts and other financial information.[5]

According to IT Chronicles, it's estimated that 300,000 new pieces of malware are created and an average of 30,000 websites are hacked every day, a speed that makes it very challenging for security systems to recognize the newest threats.[6] With the advent of ransomware-as-a-service (RAAS)—which allows a threat group to purchase a ransomware package much like any other legitimate software-as-a-service (SaaS) solution—the production of new types of ransomware has increased.

Security validation can help determine the effectiveness of security controls—how well they find and block ransomware attacks before they cause significant damage. It is critical to continuously test security controls with the emulation of real attack binaries using the tactics, techniques, and procedures, (TTPs) of malicious actors. This lets companies see how their security controls behave under actual attack conditions.

With the rapid frequency and destructive impact of ransomware attacks, Mandiant is helping organizations proactively address the threat of ransomware.

1 Infosecurity Magazine (October 1, 2021). Infant Fatality Could Be First Recorded Ransomware Death.
2 Bloomberg.com (June 5, 2021). Hackers Breached Colonial Pipeline Using Compromised Password.
3 Government Technology (January 6, 2022). Bernalillo County, N.M., Systems Disrupted by Cyber Attack.
4 Pcmag.com (March 1, 2022). Nvidia Confirms Company Data Was Stolen in Hack.
5 Reuters.com (April 14, 2021). NBA's Houston Rockets probing cyber attack, working closely with FBI.
6 T Chronicles (May 27, 2021). Cyber Security Statistics 2020.

Testing ransomware prevention with real ransomware attacks

The use of real attacks—the emulation of native binary code—is critical in testing the effectiveness of security controls. Many vendors offer attack simulations that are weaker versions of actual attacks; many simulations are often not identified as a threat by security controls. The use of machine learning (ML) often exacerbates this scenario.

Three Mandiant capabilities enable safe and successful testing with real ransomware attacks:

- Frontline threat intelligence that curates and prioritizes ransomware families that are relevant to your organization.
- Ability to repurpose real ransomware so it is predictable, controllable, and safe when testing enterprise security controls.
- A proven technology platform delivering Mandiant Advantage Security Validation to safely deploy and run repurposed ransomware attack binaries.

Repurposed ransomware

Mandiant applies a unique repurposing process to disarm original ransomware code so the ransomware can be controlled by Mandiant and its authenticity can be identified by cybersecurity controls. The process starts with conducting comprehensive analysis of the ransomware, implementing a repurposing process to the actual attack code, and finally developing the decryption capability.

- After fully analyzing the malware collected from the wild, the destructive tools from the ransomware are removed.
- Mandiant develops tooling to modify its data and options, as well as a decryption tool to recover encrypted files.
- Then permanent system degradation capabilities are disabled that are unsafe in a production environment.

The end result is a piece of repurposed ransomware which can be deployed safely in a customer's production environment to authentically test the effectiveness of security controls and provide security teams the understanding of whether or not they can withstand a ransomware attack.

Identification of top ransomware families

Current adversary visibility refers to threat intelligence that reveals what the attackers are doing in the moment. Security teams need this visibility to identify and prioritize the top ransomware families that an organization's security controls should be tested against. Mandiant Incident Response engagements provide this unique frontline visibility and inform Mandiant Advantage Threat Intelligence with the latest attacker TTPs and knowledge of who or what poses a threat to an organization.

Mandiant tracks more than 200 different ransomware families. Each quarter, the most active ransomware families are identified and selected for more in-depth research.
The ransomware families that pose the biggest risks are prioritized for repurposing.

Alternative approaches to combating ransomware and testing defenses

Common endpoint security technologies are designed to detect and prevent already known ransomware files and behaviors. They run in the background of computer processes, searching for code or text strings belonging to already known ransomware. If they find anything suspicious, the program rejects the files to keep the system safe. These programs are based on huge databases containing known malware files. Through signature-based technologies, machine learning and behavioral analysis, they search for known suspicious artifacts on the system.

These methods all rely on detection after ransomware has been deployed. That's a serious problem because ransomware often hides in computer systems for a long time before it is deployed. Using these common methods, it can take an organization more than 200 days to discover a piece of ransomware lurking in its computer systems.

Mandiant uses repurposed ransomware to safely run attack binaries against an organization's security controls to determine whether the organization can block that type of ransomware before an attack occurs.

Mandiant Advantage Ransomware Defense Validation

Mandiant is continually updating its awareness of ransomware families and variants and delivering that information to the Mandiant Advantage Ransomware Defense Validation subscription. Ransomware families repurposed to date in their most authentic form for Ransomware Defense Validation include CONTI, Darkside, MountLocker, Ryuk, Sodinokibi and LOCKBIT v2.0.

Ransomware Defense Validation is a safe, quick, and low-touch SaaS offering that generates accurate and timely reports on the efficacy of an organization's ransomware prevention controls. Most importantly, it provides the answer to the question many security leaders are pressed to answer: "Can we withstand the next ransomware attack?"

Mandiant's unique development and use of repurposed ransomware makes it possible to run authentic actions and behaviors in a production environment without worrying about an attack going rogue. It minimizes the risk to your systems and greatly improves your preparedness.

Why Choose Mandiant

Mandiant conducts security validation with the safe execution of real malware and ransomware attack binaries, whether repurposed or not. Mandiant Advantage Security Validation offering conducts testing with destructive attacks using a protected environment to execute code safely and authentically against production security controls to accurately validate security effectiveness. Both approaches offered by Mandiant are differentiators in the industry. Mandiant experts can provide guidance on the best approach based on a security team's unique testing requirements.

Benefits

- Increased confidence, knowing that you have tested your cyber defenses based on the latest yet completely safe ransomware.
- Deeper understanding of your ransomware risk based on Mandiant's early knowledge advantage of who is targeting your industry and peers. This is of enormous help to your security team which can move from being purely defensive to taking a more proactive strategy.
- Proactive practices give executives and board members confidence that you are actively helping to keep your organization safe from ransomware attacks.
- Automated and daily testing of your defenses using repurposed ransomware helps to continuously measure and better understand the efficacy of your ransomware prevention controls, and whether established processes and policies are working as expected before a ransomware attack occurs.
- Using automation to continuously conduct ransomware evaluations is the only way you can keep up with the speed of adversaries and the dynamic nature of attacks within today's new economy of threats, ransomware, and the emergence of ransomware-as-a-service.