A guide to combatting human-operated ransomware: Part 2

microsoft.com/security/blog/2021/09/27/a-guide-to-combatting-human-operated-ransomware-part-2/

September 27, 2021

This blog is part two of a two-part series focused on how Microsoft DART helps customers with human-operated ransomware. For more guidance on human-operated ransomware and how to defend against these extortion-based attacks, refer to our human-operated ransomware docs page.

In part one of this blog series, we described the process and execution used in our customer engagements to provide perspective on the unique issues and challenges regarding human-operated ransomware. We also explained how Microsoft's Detection and Response Team (DART) leverages Microsoft solutions to help combat this threat. In this post, we will tackle the risks of human-operated ransomware and detail DART's security recommendations for tactical containment actions and post-incident activities in the event of an attack.

Understanding the risks of human-operated ransomware

Beyond the immediate threat of file encryption, there are several additional risks associated with human-operated ransomware events, some of which may be observed well after an investigation and the removal of the threat from the network. These risks include:

1. Disruption of business operations

Immediate actions need to be taken to reduce the blast radius of a ransomware event. In these cases, disabling portions of the network may feel like a self-inflicted denial of service, but they are necessary to counter the ransomware spread. The resulting business disruption

may become public. If any affected systems are public-facing, it may require crisis communications.

2. Data theft

Most attackers are highly motivated to monetize their access to your network. In several cases investigated by DART, an attacker has performed reconnaissance for sensitive files (like contracts, financial documents, and internal communications), copied this data, and exfiltrated it before any ransomware was dropped. Taking this information before ransomware is deployed allows the attacker to have data to sell, leak, or simply show as proof that the attacker has had access to sensitive files.

3. Extortion

Data theft by ransomware operators opens an organization to extortion. It is not uncommon for threat actors to demand payment to prevent the leak of stolen data. These threats are typically sent via email with sample stolen documents attached as proof of possession. In some cases where DART has observed this activity, a threat actor accessed a cloud-based email account that was not protected by multifactor authentication (MFA) and sent threatening emails to the board of directors. The threat of extortion is still high, even when the threat actors are unsuccessful at deploying ransomware.

At DART, we often get asked, “Can you tell us which data was stolen?” To prove this requires concrete evidence, which would be either:

> A network capture that shows the actual data leaving the network (which rarely exists).

Or

> Finding the data outside the organization’s network, typically on a public file-sharing site. A log file showing ‘x’ bytes were transferred does not prove what data was stolen, and a command line history or event log showing a file archiving utility was run does not prove that data was stolen.

4. Follow-on attacks

To further their monetization efforts, attackers are also often observed deploying coin miners in compromised networks. This is a low-effort method to generate additional income from a victim organization when data theft or extortion are insufficient for the attacker. Depending on the attacker’s motivation, additional malware may be deployed that would allow other criminals to gain access to the environment. This access is monetized, and the sale of compromised network access is common in most human-operated ransomware cases, performed after the primary attacker has obtained what they initially sought.

5. Reputational damage

The risk of brand damage reputation is difficult to assess in the aftermath of a human-operated ransomware event. The reputation of an organization's brand may include lost customer and shareholder trust and loyalty, as well as current and future business. The risk of brand damage reputation is difficult to assess in the aftermath of a human-operated ransomware event. Reputational damage may be more costly and require longer-term solutions than the response to the human-operated ransomware event.

6. Compliance and regulatory reporting

Potential reporting requirements are another organizational risk depending on the industry or affiliation. This may include compliance or regulatory reporting in cases where sensitive financial information or personally identifiable information (PII) is stolen. Fines and loss of accreditation may further damage an organization's reputation.

Recommendations and best practices

Containment

Containment can only happen once we determine what needs to be contained. In the case of ransomware, the adversary's goal is to obtain credentials that allow administrative control over a highly available server and then deploy the ransomware. In some cases, the threat actor identifies sensitive data and exfiltrates it to a location they control.

Tactical recovery will be unique for each customer and tailored to the customer's environment, industry, and level of IT expertise and experience. The steps outlined below are recommended for short-term and tactical containment steps your organization can take. To learn more about securing privileged access for long-term guidance, visit our securing privileged access docs page. For a comprehensive view of ransomware and extortion and how to protect your organization, you can refer to our human-operated ransomware docs page.

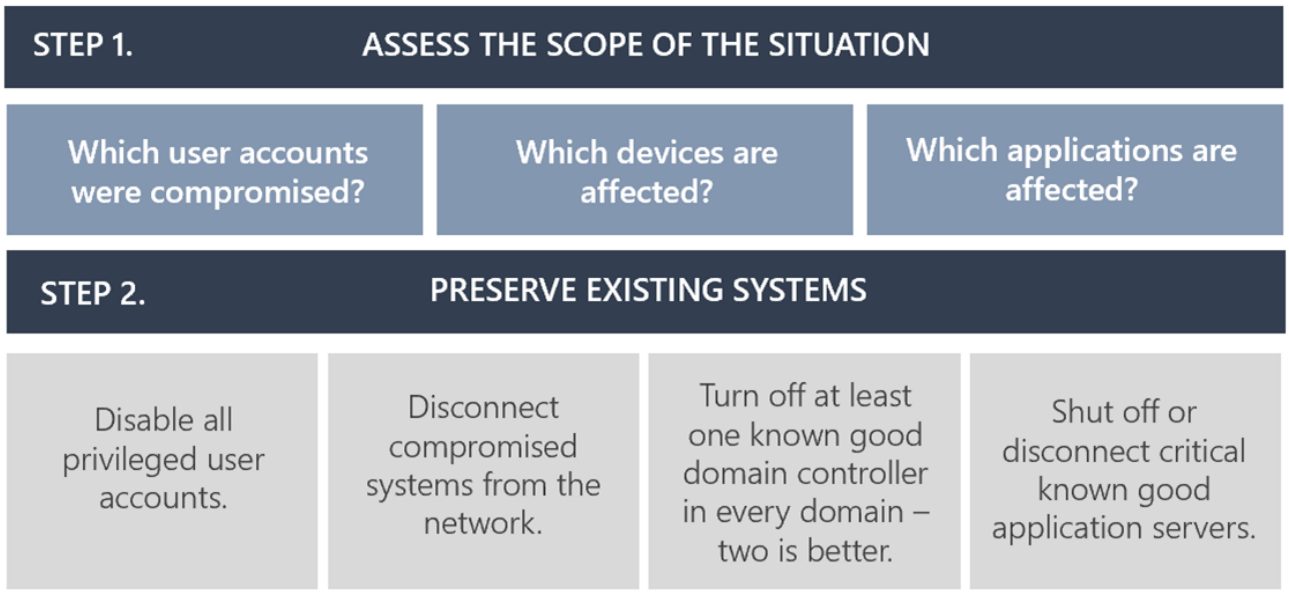

Figure 1. Containment steps that can be done concurrently as new vectors are discovered.

After the first step of containment (assessing the scope of the situation), the second step is to preserve existing systems:

- **Disable all privileged user accounts** except for a few accounts used by your admins to assist in resetting the integrity of your Active Directory infrastructure. If a user account is believed to be compromised, disable it immediately.
- **Isolate compromised systems from the network**, but *do not* shut them off.
- **Isolate at least one known good domain controller in every domain—two is even better**. Either disconnect them from the network or shut them down entirely. The object here is to stop the spread of ransomware to critical systems—identity being among the most vulnerable. If all your domain controllers are virtual, ensure that the virtualization platform's system and data drives are backed to offline external media (*not* connected to the network) in case the virtualization platform itself is compromised.
- Isolate critical known good application servers (for example SAP, configuration management database (CMDB), billing, and accounting systems).

These two steps can be done concurrently as new vectors are discovered. Disable those vectors and then try to find a known good system to isolate from the network.

Other tactical containment actions can be accomplished:

- Reset the krbtgt password, twice in rapid succession. Consider using a scripted, repeatable process. This script enables you to reset the krbtgt account password and related keys while minimizing the likelihood of Kerberos authentication issues being caused by the operation. To minimize potential issues, the krbtgt lifetime can be reduced one or more times prior to the first password reset so that the two resets are done relatively quickly. NOTE**:** All domain controllers that you plan to keep in your environment *must* be online.
- Deploy a Group Policy to the entire domain(s) that prevents privileged log on (Domain Admins) to anything but Domain Controllers and privileged administrative-only workstations (if any).
- Install all missing security updates for operating systems and applications. Every missing update is a potential threat vector that adversaries can quickly identify and exploit. Microsoft Defender for Endpoint's Threat and Vulnerability Management provides an easy way to see exactly what is missing—as well as the potential impact of the missing updates.
    - For Windows 10 (or higher) devices, confirm that the current version (or n-1) is running on *every* device.
    - Apply attack surface reduction (ASR) rules to prevent malware infection.
    - Enable all Windows 10 security features.
- Check that every external facing application, including VPN access, is protected by multifactor authentication, preferably using an authentication application that is running on a secured device.
- For devices not using Defender for Endpoint as their primary antivirus software, run a full scan with Microsoft Safety Scanner on isolated "known good" systems before reconnecting them to the network.
- For any legacy operating systems, upgrade to a supported OS or decommission these devices. If these options are not available, take every possible measure to isolate these devices, including network/VLAN isolation, IPsec rules, and log on restrictions, so they are only accessible to the applications by the users/devices to provide business continuity.

DART sometimes finds customers who are running mission critical systems on legacy operating systems (some as old as Windows NT 4) and applications, all on legacy hardware. This is one of the riskiest configurations possible—not only are these operating systems and applications insecure, if that hardware fails, backups typically cannot be restored on modern hardware. Unless replacement legacy hardware is available, these applications will cease to function.

Post-incident activities

DART recommends implementing the following security recommendations and best practices after each incident.

- Ensure that best practices are in place for email and collaboration solutions to make it more difficult for attackers to abuse them while allowing internal users to access external content easily and safely.
- Follow Zero Trust security best practices for remote access solutions to internal organizational resources.
- Starting with critical impact administrators, follow best practices for account security including using passwordless or MFA.
- Implement a comprehensive strategy to reduce the risk of privileged access compromise.
    - For cloud and forest/domain administrative access, see below for an overview of Microsoft's privileged access model (PAM).
    - For endpoint administrative management, see below for details on the local administrative password solution (LAPS).
- Implement data protection to block ransomware techniques and to confirm rapid and reliable recovery from an attack.
- Review your critical systems. Check for protection and backups against deliberate attacker erasure/encryption. It's important that these backups are periodically tested and validated.
- Ensure rapid detection and remediation of common attacks on endpoint, email, and identity.
- Actively discover and continuously improve the security posture of your environment.
- Update organizational processes to manage major ransomware events and streamline outsourcing to avoid friction.

Privileged access model (PAM)

Using the privileged access model (formerly known as the tiered administration model) enhances Azure AD's security posture. This involves:

- Breaking out administrative accounts in a "Planed" environment—one account for each level, usually four:
    - Control Plane (formerly Tier 0): Administration of Domain Controllers and other crucial identity services (like Active Directory Federation Service (ADFS) or Azure AD Connect). This also includes applications that require administrative permissions to Active Directory, such as Exchange Server.
    - The next two Planes were formerly Tier 1:
        - Management Plane: Asset management, monitoring, and security.
        - Data/Workload Plane: Applications and application servers.
    - The next two Planes were formerly Tier 2:
        - User Access: Access rights for users (such as accounts).
        - App Access: Access rights for applications.

- Each one of these Planes will have a separate administrative workstation for each Plane and will only have access to systems in that Plane. Other accounts from other Planes will be denied access to workstations and servers in the other Planes through user rights assignments set to those machines.
- The net result of the PAM is that:
    - A compromised user account will only have access to the Plane it is a part of.
    - More sensitive user accounts will not be logging into workstations and servers with a lower Plane's security level, thereby reducing lateral movement.

Local Administrative Password Solution (LAPS)

By default, Microsoft Windows and Active Directory have no centralized management of local administrative accounts on workstations and member servers. This usually results in a common password that is given for all these local accounts, or at the very least in groups of machines. This enables would-be attackers to compromise one local administrator account, and then use that account to gain access to other workstations or servers in the organization.

Microsoft's Local Administrator Password Solution (LAPS) mitigates this by using a Group Policy client-side extension that changes the local administrative password at regular intervals on workstations and servers according to the policy set. Each of these passwords are different and stored as an attribute in the Active Directory computer object. This attribute can be retrieved from a simple client application, depending on the permissions assigned to that attribute.

LAPS requires the Active Directory schema to be extended to allow for the additional attribute, the LAPS Group Policy templates to be installed, and a small client-side extension to be installed on every workstation and member server to provide the client-side functionality.

Download LAPS from the official Microsoft Download Center.

Harden your environment

Each ransomware case is different and there is no one-size-fits-all approach. But there are things you can do now to harden your environment and prepare for a worst-case scenario. Although, these changes may impact how your organization currently works, consider the risk of not implementing them now versus dealing with a potential human-operated ransomware event. An organization that has fallen victim to a ransomware attack should keep the crucial human element in mind—real people are responding to the incident at the end of the day.

Learn more

Want to learn more about DART? Read our past blog posts.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.