Ransomware Assessment Report

Purple Team and Tabletop Exercises

Prepared for

[REDACTED]

[DATE]

OSec LLC : 122 East 42nd St, New York, NY 10168 : www.OSec.com

1 Executive Summary

Between [DATE] to [DATE], OSec engaged with members of the [REDACTED] information security team to perform a Purple Team Assessment of the current ability to detect, mitigate for, respond to, and recover from ransomware incidents. This assessment included a simulated attack scenario performed by members of OSec that mimicked actions by a nefarious actor carrying out ransomware commands on a laptop provided by [REDACTED]. The outcome of this effort is the presentation of specific actions taken by the OSec team and what was detected by [REDACTED]and associated security vendors.

On [DATE], the group met to participate in the Purple Team ransomware exercises. The objective of the exercise was to present the [REDACTED] team with a ransomware scenario on a laptop provided by them and record and evaluate their detections. At the outset of the exercise, guidelines were established to encourage a conversant and collaborative approach to responding to the attack. Overall, while informal, the response to the exercise was well-handled and had clear direction.

The Incident Response Tabletop was held on [DATE] between the OSec and [REDACTED] teams. The goal was to present a plausible ransomware scenario to the [REDACTED] team and evaluate their current response capabilities in a low risk and collaborative environment. There were several strengths and weaknesses identified and detailed further in this report. The [REDACTED] team showed good organization and general approach to incident response, but have room for improvement, particularly in improving the organization's incident response capability's maturity and filling some identified gaps.

As evidenced from this exercise and other conversations OSec has had with various stakeholders across the organization, [REDACTED] has developed and deployed a strong baseline infrastructure to support its operations and keep the environment secure. The evidence provided in this report will further advance the maturity and resiliency of the [REDACTED] security landscape and help to inform future policy decisions and development.

2 Findings Summary

While the [REDACTED] team and associated vendors detected certain nefarious commands and objectives, the assessment confirmed that the detection types and timeliness could be improved.

The allowance for every user to have local Administrator rights is also a concern; the OSec team was able to install a virtual machine from which to launch attacks inside the [REDACTED] network unfettered by defenses.

3 Scenarios

The main goal of the exercise was to evaluate how detection worked against a simulated ransomware threat in the [REDACTED] working environment. The scenario employed techniques that could be used to lock [REDACTED] employees and contractors out of their working environment with ransomware, restricting the ability to service specific endpoints.

4 Mitre ATT&CK Framework Mapping

The techniques and sub-techniques that were attempted are the following ransomware-associated Tools, Techniques, and Procedures (TTP) from the MITRE ATT&CK Framework:

- T1083: File and Directory Discovery
- T1140: Deobfuscate/Decode Files or Information
- T1027: Obfuscated Files or Information
- T1135: Network Share Discovery
- T1057: Process Discovery
- T1049: System Network Connections Discovery
- T1016: System Network Configuration Discovery
- T1033: System Owner/User Discovery
- T1106: Native API
- T1486: Data Encrypted for Impact

- T1041: Exfiltration Over C2 Channel
- T1567.002: Exfiltration to Cloud Storage
- T1490: Inhibit System Recovery
- T1485: Data Destruction
- S0105: dsquery
- T1543.001: Create or Modify System Process
- T1564.006: Hide Artifacts: Run Virtual Instance
- S0521: Bloodhound: Active Directory (AD) reconnaissance tool

5 Scenario Execution

The main component of this assessment was to review how the [REDACTED] team and its associated security vendors detect and mitigate ransomware activity. This was accomplished by obtaining a laptop along with VPN and Zscaler credentials from [REDACTED] for OSec to perform ransomware related attacks from.

From the Red Team perspective, an indication of “Success” means that the command was able to execute with intended results.

The Purple team engagement was performed over the course of two sessions of two hours on [DATE].

As all users are granted local Administrator privileges, the Red Team’s Techniques were executed with this authorization as well.

5.1 Red Team Perspective

Session 1: 08:00AM EST

- 08:31 AM - **T1083: File and Directory Discovery** - Success

[REDACTED]

- 08:35 AM - **T1140: Deobfuscate / Decode Files or Information** - encode Success, decode Fail

[REDACTED]

- 08:54:02 AM - **T1027: Obfuscated Command in PowerShell** - Success

[REDACTED]

- 08:55:31 AM - **T1135: Network Share Discovery** - Success

[REDACTED]

- 08:56:34 AM - **T1057: Process Discovery** - Success

[REDACTED]

- 08:58:10 AM - **T1049: System Network Connections Discovery** - Success

[REDACTED]

- 08:58 AM - **T1016: System Network Configuration Discovery** - Success

[REDACTED]

- 09:01 AM - **T1033: System Owner/User Discovery** - Success

[REDACTED]

- 09:14 AM - **T1106: Execution through API** - Success

[REDACTED]

Figure 1 - Calc was Executed through API

- 09:27:48 AM - **T1486: Data Encrypted for Impact - Simulate AES Encryption** - Success

[REDACTED]

Your FAKE important data have been really encrypted by a FAKE OSec Ransomware!
So nothing is lost, it is just a Purple Team exercice.
Contact the POC if you find this file, or try to find out more...

No need to send bitcoins!

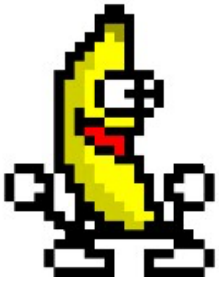

Figure 2 - Ransomware Page Displayed after Encryption

- 09:16:30 AM - **T1041: Exfiltration over C2 Channel** - Success

A request to send data to 'http://example.com ' was a success as shown highlighted below on line 5 and 6: 200 and OK.

[REDACTED]

- 09:18:36 AM - **T1567.002: Exfiltration to Cloud Storage (User/**[REDACTED] **Controlled OneDrive)** - Success

Documents exfiltrated to User's OneDrive folder named Exfil. Members of OSec who were a part of this engagement were invited to the OneDrive folder named Exfil, these were email addresses outside of the [REDACTED] network.

[REDACTED]

Figure 3 - Inviting OSec Email to the Internal [REDACTED] OneDrive

- 09:29 AM - **T1490: Inhibit System Recovery - Delete Volume Shadow Copies** - Fail

[REDACTED]

- 09:30 AM - **T1485: Data Destruction - Overwrite Deleted Data on C Drive** - Success

As indicated below where the output says "Writing 0x00", the process is overwriting deleted data. The process was stopped before it could complete.

[REDACTED]

- 09:45 AM - **S0105: dsquery**

The Red Team was unable to install the dsquery command line tool due to system restrictions, however they were able to run the tool from a USB drive extracting known hosts connected to the Active Directory.

[REDACTED]

Figure 4 - dsquery Execution from External USB Drive

[REDACTED]

Figure 5 - Output from dsquery Formatted for Scanning with Nmap and SMBMap

- 09:51 AM - **T1543.001: Create or Modify System Process: Launch Agent** - Fail

Attempts to launch a C2 agent were unsuccessful as shown below by the response, `This script contains malicious content and has been blocked by your antivirus software.`

[REDACTED]

- 09:55 AM - **S0521: Bloodhound: Active Directory (AD) reconnaissance tool** - Fail

The Active Directory tool known as Bloodhound which aids in penetration testing and privilege escalation was downloaded. However CrowdStrike detected its use upon execution.

[REDACTED]

Figure 6 - Bloodhound Tool Denied Access by CrowdStrike

Session 2: 10:30PM EST

- 10:38:04 PM - **T1083: File and Directory Discovery** - Success

[REDACTED]

- 10:41:12 PM **T1027: Obfuscated Command in PowerShell** - Success

[REDACTED]

- 10:45 PM - **T1106: Execution Through API** - Success

[REDACTED]

Figure 7 - Calc was Executed through API

- 10:46:09 PM - **T1486: Data Encrypted for Impact - Simulate AES Encryption** - Success

[REDACTED]

Your FAKE important data have been really encrypted by a FAKE OSec Ransomware!
So nothing is lost, it is just a Purple Team exercice.
Contact the POC if you find this file, or try to find out more...

No need to send bitcoins!

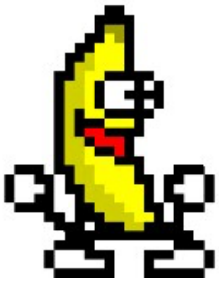

Figure 8 - Ransomware Page Displayed after Encryption

- 10:50:20 PM - **T1567.002: Exfiltration to Cloud Storage (External Controlled Dropbox)** - Success

Dropbox was installed. The same operation that was performed at 09:18:36 AM, except with a Dropbox folder, was completed successfully.

[REDACTED]

Figure 9 - Dropbox Installed and [REDACTED] Laptop with Exfiltrated Data

[REDACTED]

Figure 10 - Exfiltrated Data on Externally Controlled Dropbox Folder (on External Computer)

- 10:53 PM - **T1485: Data Destruction - Overwrite Deleted Data on C Drive** - Success

As indicated below, where the output says “Writing 0x00”, the process is overwriting deleted data. The process was stopped before it could complete.

[REDACTED]

- 11:02:39 PM - **T1041: Exfiltration Over C2 Channel** - Success

A request to send data to 'http://example.com ' was a success as shown highlighted below on line 5 and 6: 200 and OK.

[REDACTED]

- 11:15PM - **T1564.006: Hide Artifacts: Run Virtual Instance** - Success

As CrowdStrike was inhibiting our ability to install a C2 agent or run typical hacking tools, the decision was made to try to run those in a virtual environment to bypass protections.

VirtualBox was installed as the user has local Administrator rights. Pop_os (Ubuntu variant) was loaded as a guest operating system. Nmap and SMBMap which are used to scan a network for open ports and shares were installed within the guest OS without being detected by CrowdStrike or other defenses. OSec was able to scan the internal network for open ports and open shares using standard tools that would normally get flagged by CrowdStrike.

[REDACTED]

Figure 11 - VirtualBox Running on [REDACTED] Laptop with Hacking Tools Running

Notes:

- The Red team also attempted to download various files from network shares and store them in the Dropbox and OneDrive folders, all of these were completed successfully.
- Local Administrator rights allowed for the installation of virtual machines and allowed access to execute functions that would normally be disallowed.
- Having Zscaler operational during the second session did not seem to change the outcome of technique execution.
- The Red Team is not sure if detections would have been noticed if the Blue Team wasn't actively watching the CrowdStrike Console
- Dsquery was able to run on the host machine via an external USB drive and the Red Team was able to procure a list of internal hosts from the Active Directory.

5.2 Blue Team Perspective

- 9:34:24 AM, CrowdStrike recorded a critical severity detection when the process [vssadmin.exe] attempted to delete all shadow copies via the command line [vssadmin.exe delete shadows /all /quiet] on the host [REDACTED]. The user attributed to this detection was [REDACTED]. This activity was blocked in CrowdStrike and remediation was performed by the Falcon Complete team.
- 9:35:25 AM, CrowdStrike detected the use of Cipher.exe to overwrite deleted data, warns "Adversaries may delete files left behind by the actions of their intrusion activity."
- 9:56:40 AM CrowdStrike detects an executable run with an argument of sysvol.
- 7:11:09 PM CrowdStrike detected a process with an obfuscated command line appears to be using certutil to decode a malicious payload.
- 7:59:03 PM CrowdStrike detected the deletion of backups often indicative of ransomware activity - AESCipher.txt; vssadmin.exe; dsquery.exe; T1083-Output.txt; my_important_fake_file.doc; Key.txt; README_decrypt.html; LineNumbers.txt; Example Domain ; Untitled1.ps1; Purple Documentation.txt; cipher.exe;
- 8:02:00 PM, CrowdStrike detected "A process gathered information about the operating system or hardware. Adversaries can use this to identify system vulnerabilities." - nslookup; results.txt; nbtstat, arp, netsh, ipconfig, whoami; dsquery; net1.exe;

- 8:15:52 PM, CrowdStrike detected “A process gathered information about the operating system or hardware. Adversaries can use this to identify system vulnerabilities.” - Bloodhound.exe
- 8:20:00 PM CrowdStrike detected “A script launched that appears to be related to a reverse shell established with a remote system”.
- 9:42 PM, ReliaQuest/Forescout detected ANONYMOUS LOGON to [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]; login to [REDACTED]; Multiple events from Forescout mentioning Rogue Wireless device and another albeit new device with no IP assigned (possibly a VM).
- Unknown time, CrowdStrike detected unauthorized data transfer - USB Drive (D); Screenshots; [REDACTED]; [REDACTED] ;

Notes:

- Detections included are from the day of the engagement only.
- The morning engagement was run without Zscaler operational.

5.3 Purple Team Exercise Mitre ATT&CK Mapping:

Initial Access	TA0002: Execution	TA0005: Defense Evasion	TA0007: Discovery	TA0010: Exfiltration	TA0040: Impact	TA0003: Persistence
T1566.001: Spearphishing Attachment	T1106: Native API	T1140: Deobfuscate/Decode Files or Information	T1083: File and Directory Discovery	T1041: Exfiltration Over C2 Channel	T1486: Data Encrypted for Impact	T1543.001: Create or Modify System Process: Launch Agent
T1566.002: Spearphishing Link	T1569.002: System Services: Service Execution	T1027: Obfuscated Files or Information	T1135: Network Share Discovery	T1567.002: Exfiltration to Cloud Storage	T1490: Inhibit System Recovery	
T1078.002: Valid Accounts / Domain Accounts	T1053.005: Scheduled Task	T1564.006: Hide Artifacts: Run Virtual Instance	T1057: Process Discovery		T1489: Service Stop	
T1078.003: Valid Accounts /Local Accounts			T1016: System Network Configuration Discovery		T1485: Data Destruction- Overwrite deleted data on C drive	

T1189: Drive-by Compromise			T1049: System Network Connections Discovery			
			T1033: System Owner/User Discovery			
			T1082: S0521: Bloodhound: Active Directory (AD) reconnaissance tool			

Red: Security control fail as Purple Team test succeed.

Green: Security control succeeded as Purple Team test failed.

White: Untested potential ransomware tactic.

5.4 Analysis and Recommendations

The major themes that stood out during the engagement were:

- Users are granted local Administrator by default;
- Certain ransomware activity is undetected unless actively watched;
- Lack of timeliness of reporting on ransomware activities that were detected;
- Attack / ransomware tools can be run from an external device or virtual machine; *and*
- Zscaler did not seem to impact the techniques executed as well as access to certain network resources.

It is a common recommendation to disallow users to have local Administrator rights on workstations. This allowed the OSec team to run commands and install software that should have been caught or disallowed.

The techniques chosen from the MITRE ATT&CK Framework were specific to ransomware-like activity. Out of twenty-three (23) commands, three (3) were actively blocked from executing, two (2) of those were duplicate commands. After the remaining twenty (2) commands successfully executed attention was drawn to those activities based upon the blocked execution attempts, however it was not apparent that they would have been caught on their own.

Zscaler did not impact OSec activities as the only techniques detected or blocked were by CrowdStrike and manual monitoring during the second session. Whether Zscaler actually detects malicious traffic or not is unknown; it is recommended to review and test the rules set in place.

The timeliness and types of detections should be reviewed. Based upon the results of this exercise, they could be too slow and possibly miss ransomware activities.

6 Incident Response Tabletop

The Incident Response Tabletop was held on March 8th between the OSec and [REDACTED] teams. The goal was to present a plausible ransomware scenario to the [REDACTED] team and evaluate their current response capabilities in a low risk and collaborative environment.

6.1 [REDACTED] Participants

[REDACTED]

6.2 Initial Scenario

At the beginning of the scenario, the [REDACTED] team was presented with the following initial situation:

- The time is 9:00 am;
- There are 20 users who have been locked out of their AD accounts (from various departments across the organization);
- No alerts have been sent at this point from CrowdStrike or any other Blue Team feeds.

6.3 Exercise Walkthrough

9:00 AM

[REDACTED] Activities/Responses

- [REDACTED]

9:07 AM

OSec Inject: A user calls stating that there is a ransomware note on his screen. At 9:15 am, a second user has reported similar issues with a ransomware note to [REDACTED] Help Desk which prevents them from using their computer. At the appearance of the ransomware (Figure 12).

[REDACTED] Activities/Responses

- [REDACTED]

Your FAKE important data have been really encrypted by a FAKE OSec Ransomware!
So nothing is lost, it is just a Purple Team exercice.
Contact the POC if you find this file, or try to find out more...

No need to send bitcoins!

Figure 12 - Ransomware Note Provided to the [REDACTED] Team

11:30 AM

OSec Inject: Several users are now calling in seeing the same message and user lockouts have been resolved.

[REDACTED] Activities/Responses

- [REDACTED]

OSec Inject: Also, at 11:30 am, the [REDACTED] Ops team investigated some of the infected machines and came back with the following:

1. [REDACTED]

[REDACTED] Activities/Responses

- [REDACTED]

12:30 PM

OSec Inject: OSec provided feedback to [REDACTED] from their work on the incident response:

1. There is new ransomware that appears to have a similar splash screen message as has been spotted in the wild.
2. This ransomware is a polymorphic malware, not just a ransomware, and also runs other malicious functions.
3. One of them is trying to abuse lateral movement within the environment.
4. CrowdStrike has not yet provided detections regarding the activity.
5. A developer machine has been affected which has access to the [REDACTED].
6. Upon investigation, a server was discovered with the same ransomware popup reported by end users.

[REDACTED] Activities/Responses

- [REDACTED]

1:30 PM

OSec Inject: Servers are starting to display the ransomware image from Figure 12.

- OSec informs you that command and control servers (C2) have been found related to this malware.

- A malicious URL appears to have been used to exfiltrate text information from an endpoint over HTTPS to the Cloud. This is good timing, as your leadership wants to know what data has been exfiltrated, if any.
- Can you identify all endpoints that have been or are communicating to this URL and how?
- Can you find out what could have been exfiltrated?

[REDACTED] Activities/Responses

- [REDACTED]

2:45 PM

OSec Injects:

- A system admin informs the incident response team that when he connected to a server, he found an open RDP session with a command, as shown below.
- The RDP session has not been opened by a legitimate user.
- What can you do? Can you identify if any more commands have been executed on all endpoints? Can you identify all non-legitimate RDP sessions?

[REDACTED]

Figure 13 - Open RDP Session Displayed

- SSH sessions to a critical server part of [REDACTED] gateway from a Developer machine are affected as well.
- The file storage (NFS) system from the [REDACTED] shows sign of high disk activities.
- [REDACTED] is informed from the online press that [REDACTED] cloud users appear to have trouble accessing their data from mobile apps.
- [REDACTED] Domain and [REDACTED] Cloud assets have now been found to contain active Ransomware. What is the IR course of action?

[REDACTED] Activities/Responses

- [REDACTED]

3:00PM

OSec Injects:

- The team decided to follow Failover Procedures and switch to the passive instance.
- Delay and technical difficulties slow down the failover.
- What is the IR course of action?
- Is rebuilding from tape backup/original media possible?
- What is the projected time to rebuild?
- What is the communication strategy?

[REDACTED] Activities/Responses

- [REDACTED]

3:30pm

OSec Injects:

- The team closes the incident.
- Can you provide evidence with your current tools and answer leadership's questions about potential exfiltration?
- Are remote workers more of a challenge than when they are onsite?
- Globally, can you know what is happening in your network in real time and in the past?
- Do you know what is normal versus unusual?
- Are you confident with your backup/restoration process?

[REDACTED] Activities/Responses

- [REDACTED]

6.4 Analysis

Following the exercise, the OSec team reviewed notes and summarized strengths and weaknesses identified during the discussion.

Strengths:

- Communication: Each department had knowledge of who to call, when, and at what level they should be involved.
- Prompt Notification to Management: [REDACTED] knew to contact management as the situation escalated.
- Tool Proficiency: The team knows their tools and how they work.
- Areas of Responsibility: Based on the team's behavior and feedback during the exercise, each member of the team reported acting according to their current roles and responsibilities and noted having the autonomy and organizational trust to act independently (except when it came to matters involving Legal).
- Priority Users: There was mention that a different response for a 'regular' user versus a 'VIP' user would happen. In a real-world situation, there would likely be practical differences to the response.
- Containment: When the first ransomware report came in, it was decided to immediately put that machine into containment. This is important as the spread of infection to other machines could be happening.

Weaknesses:

- Evidence Collection: There was no mention of "preserving evidence" (particularly related to the infected endpoint investigation that would be performed). It is unclear if this is handled by CrowdStrike or ReliaQuest. A formal policy regarding handling evidence needs to be in place.
- Coordinated Response: While each team member displayed excellent communication, it is important to coordinate that communication into a defined method in relation to malware and ransomware specific activities.
- User Feedback: No mention was made of how to respond to end users who report a security issue. While it is understandable to want to control the information of a ransomware threat leaking to the public, this is something that should be reviewed as, at

some point, the security or communications team may need to inform users that malicious emails or executables are circulating. Communications like this could prevent additional compromise.

- Knowledge Gaps: Incident response often involves new or unknown areas. The incident response team appears to rely heavily on reports from CrowdStrike, ReliaQuest, etc. However, the team should ensure their incident response process involves research and investigation of unknown situations and proper management thereof. This could include looking at the MITRE ATT&CK framework or other standards and then elaborating on potential mitigation.
- Spread: There was a considerable amount of time spent looking at each machine that was already known to contain ransomware to see what tools were installed etc. However, after quarantining the known ransomware machine, time should be spent preventing the spread of ransomware instead of finding out exactly what the malicious users were doing on the ransomware machine.

7 Overall Assessment and Conclusion

OSec performed a Purple Team Assessment of the current ability of [REDACTED] to detect, mitigate for, respond to, and recover from ransomware incidents. OSec also moderated a Tabletop exercise with key stake holders with a focus on ransomware within the [REDACTED] environment and how it is handled.

Overall, the OSec team concludes that, while the [REDACTED] team repeatedly demonstrated knowledge of how to delegate responsibility and the appropriate steps to be taken upon ransomware activity, there needs to be a unified response plan that is practiced regularly in a Red, Blue, or Purple Team engagement. The reliance upon third party vendors to catch ransomware-like activity is limiting and needs to be investigated as to why certain activity is not detected.

[REDACTED] has sufficient tooling in place to cover exposure areas such as email and malicious process detections, however it is apparent that those tools need to be fine-tuned or have specific rules set in place to catch real ransomware activity. As mentioned previously, giving every user Local Administrator rights is a large exposure risk and this should be a priority to remedy.

Following the recommendations outlined in this report will improve the incident response capabilities and overall maturity of the security program. Additionally, [REDACTED] should consider:

1. Plan Red Team/Blue Team or Purple Team exercises in order to validate incident response tools, processes, and environment changes as a result of this assessment in a “real drill” incident response exercise.
2. Investigate why certain techniques performed in this engagement are not detected by their security vendors unless actively monitoring the host and determine what the ‘time to detection’ is on the techniques that they are catching. Overall, it appears that the [REDACTED] team in charge of handling alerts is not seeing them until possibly too late.
3. Plan to migrate users from a Local Administrator account to a user account with only the privileges that they need.
4. Investigate access allowed to internal network with Zscaler operational vs turned off.
5. Disallow sharing of internal OneDrive folders to external emails.
6. Disallow external cloud file sharing programs, such as Dropbox.

7. Disallow external devices such as USB and investigate why CrowdStrike detected unauthorized file transfers to a USB yet did nothing to stop it.
8. Formulate a coordinated response plan that is exercised.
9. Formulate a disclosure and communications method or template and integrate it into the Incident Response Plan.

The recommendations provided in this report are meant to address issues that will result in immediate improvement in the organization's security posture and additional insight to day-to-day operations. [REDACTED] should evaluate the recommendations provided in this report and then develop a strategy to implement the appropriate improvements based on the business's needs and resources.