INCIDENT RESPONSE PLAYBOOK FOR BLACKSUIT AND PHOBOS RANSOMWARE ATTACK

Alida Øvermo-Mortensen

Delivered as part of Bachelor thesis

Contents

Introduction

This incident response playbook was created to demonstrate a possibility for practical implementation of the results from the bachelor research project. The bachelor project aimed to analyse two samples of **Blacksuit** and **Phobos** ransomware by replicating the Hybridized Comparative malware analysis framework (Schmitt, 2019) adapted to use cloud-based sandboxes. The playbook is built around the common IOCs identified by analysing **Blacksuit** and **Phobos** ransomware according to the methodology outlined in chapter 3 of the bachelor thesis.

This playbook outlines the steps that can be taken to identify and respond to an attack by **Blacksuit** or **Phobos** ransomware. The workflow for this playbook has been designed to be applicable for both ransomware families.

The incident response process is based on the SANS incident response framework in figure 1.

SANS Incident response lifecycle

SANS has developed an incident response framework. It contains six general steps to be implemented in the incident handling process. The framework can be used to respond to any incident or as a template for creating specific incident response plans or playbooks. The six phases are briefly described further:

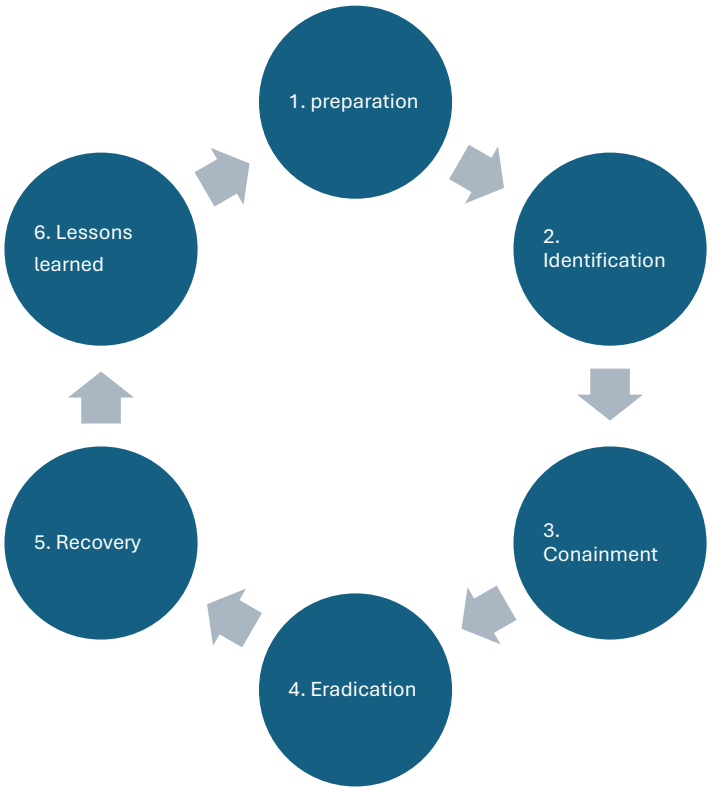

Figure 1 – Illustration of the six steps in the SANS incident response lifecycle

1. **Preparation**
   This phase involves making sure the business has all the requirements for handling a cyber incident. An incident is described as any interruption to normal business operations. Without a specified team and delegated responsibilities, the business will not be able to respond effectively to an incident.
   This phase also involves putting in place the log sources and monitoring systems required to perform effective incident response.
2. **Identification**
   The phase refers to the detection of the incident, and the steps taken to confirm an incident has occurred. An incident is often detected by looking for anomalies in log

sources or network monitoring. Employees experiencing encrypted or malfunctioning devices can be the first detection of a ransomware attack.

3. **Containment**
   The phase refers to determining the extent of the incident and taking the first remediation steps to limit further damage and lateral movement. Short-term containment is implemented, which are steps taken not as the final solution to the problem but to limit further damage and to allow business operations to continue despite the interruptions.
4. **Eradication**
   Removal of malware and redeployment of infected systems. Permanently removing the threat. This phase focuses on identifying the root cause of the incident and eradicating it.
5. **Recovery**
   Recovery includes any steps required to recover to normal business operations. This often involves testing and monitoring for infection. It is important to verify that compromised systems are fully restored and clean from malware.
6. **Lessons learned**
   The phase involves properly documenting the incident in order to improve the process and to assess the damage. As seen in the illustration of the SANS incident response lifecycle, this phase is referring to the preparation phase. It means that the lessons learned of the incident should be used to prepare for incidents better in the future and prevent them from happening.

(Kral, 2021)

The steps are generalized to fit all incidents and ensure required personnel, policies and processes are in place prior to an eventual incident.

The incident: Phobos or Blacksuit ransomware attack

Ransomware is malicious software that encrypts the files on the victim's system and demands a ransom for the decryption key needed to restore the data. The data is held for ransom on the victim's machine. A ransomware attack might also extend to include data extraction. In a double-extortion attack, an additional ransom is demanded to avoid public disclosure of the stolen data (National Cyber Security Centre, 2024).

Phobos and **Blacksuit** are two distinct encryption-type ransomware families. Various infection vectors have been observed in the wild. Phishing emails with malicious attachments is a common infection method. The use of stolen credentials, which can be used for devices where Remote Desktop Protocol (RDP) is enabled is another possibility. Software vulnerabilities allowing malicious downloads has also been used in attacks in the wild (Cybersecurity & Infrastructure Security Agency, 2024).

After the initial infection, the ransomware will perform system discovery. It will inhibit system recovery by deleting volume shadow copies. Phobos will write itself to the startup directory for persistence.

Within minutes of infection, the ransomware will encrypt all files on the computer. Furthermore, it will attempt lateral movement over the local network to encrypt more endpoints. An effective and active detection and response plan is crucial to stop the ransomware attack before it reaches the encryption phase. An example of an attack process can be seen in Figure 2.

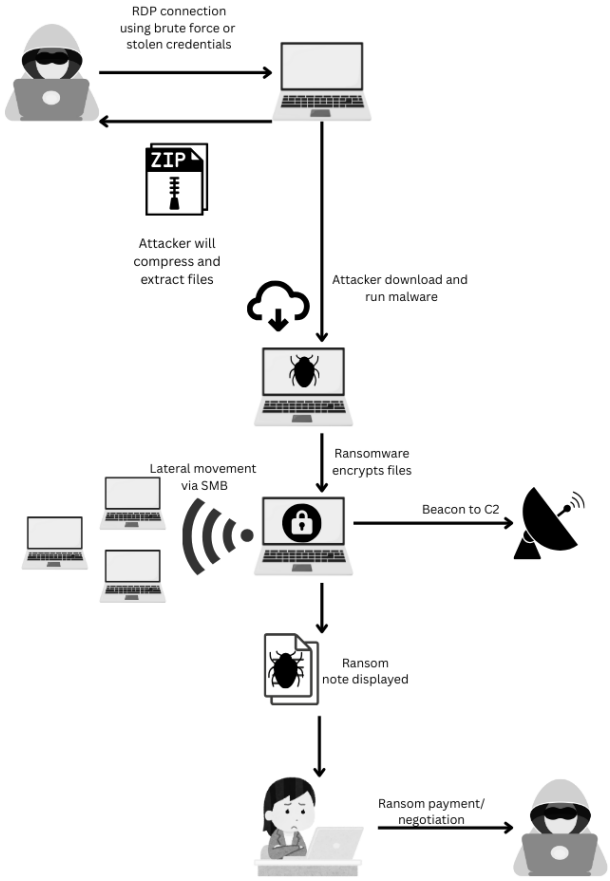

Figure 2 – Attack process

While the initial infection vector may vary, figure 2 displays an attack flow where the initial infection is caused by the attacker using RDP. This initial access method is seen in attacks by both **Blacksuit** and **Phobos**. The RDP connection is typically secured with a username and password. The credentials can be obtained by the attacker by brute-forcing, social engineering, phishing, or bought from initial access brokers from the dark web. With access to the system, the attacker can download and execute the ransomware on the victim system.

After getting access to the system, the threat actor will often perform data exfiltration of the valuable files before executing the ransomware. This is to threaten the victim with public exposure of the data on the ransomware group's leak site if ransom is not paid. This is called a double-extortion attack. Common tools to use for data compression and exfiltration are legitimate windows tools such as g-zip or rclone to avoid detection. The penetration testing

tool Cobalt strike has also been observed used for remote access and data exfiltration in **Blacksuit** ransomware attacks. As **Phobos** is used as a RaaS (Ransomware-as-a-Service) by many different and unrelated threat actors, inconsistent choice of tools is expected. However, both ransomware families compress the data before extraction.

The ransomware file will then be executed and encrypt the files on the system. **Blacksuit** will attempt lateral movement using SMB. This is a protocol used to share files on a local network. Lateral movement by SMB is not observed in **Phobos** attacks. **Phobos** will connect to a malicious domain (depicted as beacon to C2) to inform of successful infection of the machine. No such beacon behaviour is observed in **Blacksuit** ransomware attacks.

A ransom note is then displayed with contact information and instructions for the victim on how to pay the ransom. It often must be paid in cryptocurrency. The victim is depicted paying the ransom according to instructions, in the hope of receiving a decryption key to restore their files.

Incident response process

The SANS framework is used as a general template for this playbook, which is tailored for incidents caused by ransomware attack from **Phobos** and **Blacksuit** ransomware.

A graphical representation of the incident response process can be seen in figure 3.

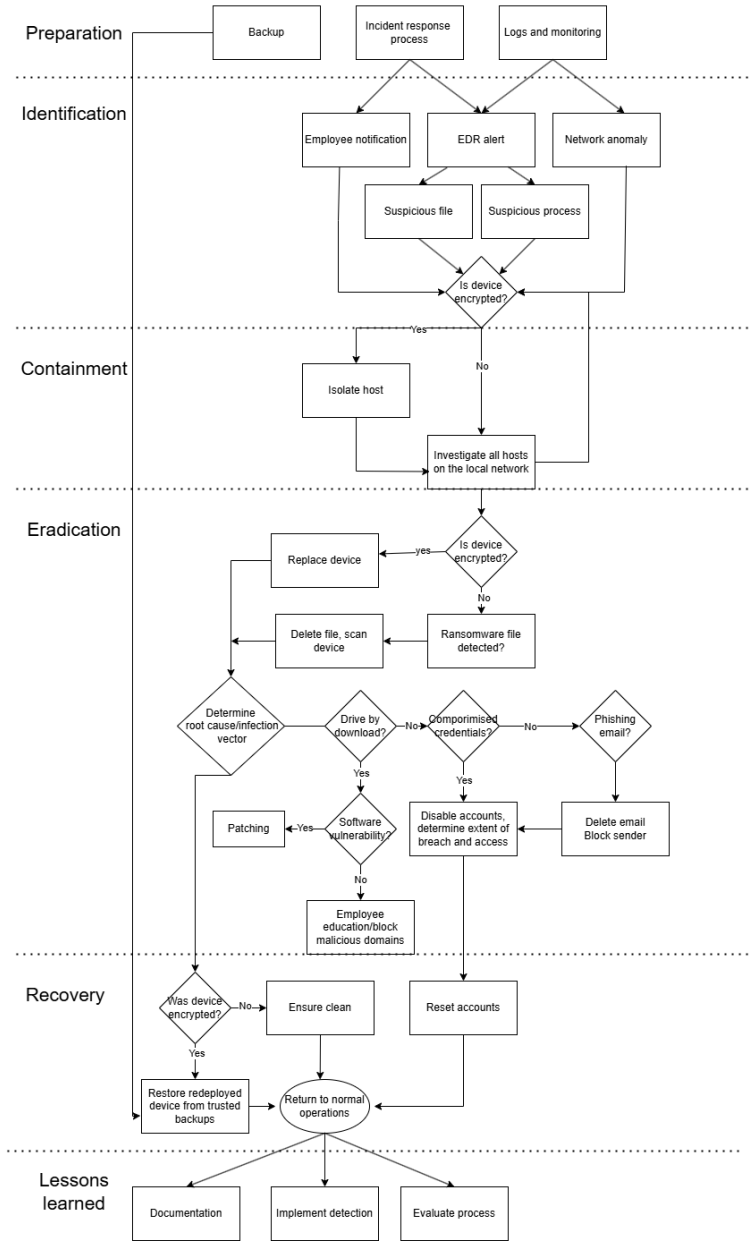

Figure 3 - Incident response flowchart

The **preparation** depicted includes fundamental concepts of security that should be implemented in an organization. The details of how this is implemented may vary depending on the business context. To be able to recover from a ransomware attack without paying the ransom, and to be able to continue normal operations in the case of systems down, having a backup plan implemented is crucial. In Figure 3, this part of phase 1 **preparation** is what allows for phase 5, **recovery**, to be performed successfully.

The **preparation** includes having the necessary **logging and monitoring systems** to be able to **identify** the ransomware attack in phase 2.

After the attack has been identified by either of the three options presented in Figure 3 or a variation of the three options listed, the incident response moves to phase 3 **containment**. The next action depends on the state of the identified infected machine. **Containment** involves investigating all hosts on the network for infection and isolating the device if necessary. The goal is to limit the ransomware from spreading, and to determine the extent of the attack.

When all infected devices have been located and isolated if needed, the **eradication** phase is initiated. To ensure the attacker loses access to the system, the initial infection vector must be identified. The most observed options for **Phobos** and **Blacksuit** are suggested in the flowchart, with recommendations for **eradication** steps according to each infection vector. In the case of a phishing email being the root cause of the attack, this often includes that the victim provided their credentials or session to the attacker. Therefore, this option is linked to the stolen credentials action in the flowchart.

The recovery phase includes long-term solutions to return to normal operations. If the business had a functioning backup system implemented in step 1 preparation, this can ideally be achieved by recovering the encrypted files from the backup. If the attack included compromised credentials, these must be addressed as seen in the flowchart in addition to handling the encrypted devices.

It is recommended to learn from the incident by developing new detection rules based on the knowledge and findings, as well as improving the incident response process itself. The last step **lessons learned** in the SANS Incident response framework can be implemented many ways, but systematic documentation and review of the incident process is key.

The proposed incident response process can be used as a general approach to ransomware attacks caused by different encryption-type ransomware families. Each step in the incident response workflow will be explained in detail in the next section, including the specifics for the ransomware families **Phobos** and **Blacksuit**.

1. Preparation

1.1 Backup plan

To be able to recover from a ransomware attack without paying the ransom, the business must have implemented a backup plan for critical assets and services. Depending on the location and type of asset, this needs to be tailored to the business. Best practice involves having backup according to the 3-2-1 rule:

- 3 backups in total
- 2 different storage media
- 1 offline

(NCCoE, 2023)

In the case of ransomware which often attempts lateral movement to delete backups stored other places in the same network, having a backup stored air-gapped or at least on a segmented network is crucial.

Devices crucial for business operations should be redundant. If they are infected with ransomware and rendered useless, a backup device can perform the same service to ensure business continuity.

Good network segmentation can help significantly in limiting the extent of a ransomware attack. Crucial assets should be isolated from exposed devices on the network.

1.2 Data points to collect

To perform effective incident response, certain monitoring systems and log sources need to be in place. The following is a non-exhaustive list with systems that act as sources of evidence in an incident:

- Network monitoring within the local network
- Firewall logs of outgoing DNS requests
- Process monitoring on endpoints
    - Any detection of processes performing the registry reads and command line listed in section 2.2 should be automatically blocked and generate an alert so that it can be investigated. Automation of blocking processes is necessary because the ransomware is reaching the encryption phase of execution very fast (<2 minutes)
- System event logs
- Email filters and options to scan attachments before potential download

1.3 YARA rules

The YARA rules references to in the playbook can be downloaded from the following GitHub repository: https://github.com/alovmo/YARA-rules

YARA rules are widely adopted detection rules used to identify malware. They are supported by many vendors and can be written in a normal text editor. The YARA rule consists of statements that if true, will mean the file matched the criteria and triggered the rule. YARA can be written to search for certain strings in a file or trigger on metadata on the file. The rules in the provided GitHub repository contain YARA rules to detect **Phobos** and **Blacksuit** ransomware.

2. Identification

The **Phobos** and **Blacksuit** ransomware is capable of encryption of the victim machine within **1 minute**. This was observed in the sandbox analysis. That means if the ransomware is allowed to execute, it is urgent to detect and block it in time.

The identification of a ransomware attack can happen in different ways which is elaborated further in this section.

2.1 Detection of possibly malicious file

When a file is downloaded, it is by default placed in the **Downloads** folder. If malware has recently been downloaded on the system, it will likely be placed here. This folder or any downloaded files could therefore be scanned with the YARA rule *phobosandblacksuit.yara* to detect files that potentially are **Phobos** or **Blacksuit** ransomware. The rule can also scan email attachments. This is relevant as a potential initial infection vector is malicious attachments sent via email.

The YARA rule triggers if the file imports the unusual function sleep() in the DLL kernel32. This function is often used to perform detection evasion by delaying execution. The function is rarely used by benign files, as more safe alternatives exist to control program timing. The YARA rule checks the file's entropy as well. High entropy means a file is likely packed, which is another method for detection- and analysis evasion. The study revealed both **Phobos** and **Blacksuit** contained these characteristics.

Possible false positives of the rule include IDEs and software developer tools. These might be packed and often include the function sleep() to provide the function to the developer. Other possible false positives include video games executables as they often contain the function to control timing.

If the YARA rule is triggered for a file, the file should be assumed to be malicious. It must be prevented from executing and preserved for further analysis in a sandbox environment. The SHA256 sum of the file should be calculated and used for threat hunting in the containment phase. Store the SHA256 sum in the YARA rule *yararulehash.yara*. This rule can be used to scan directories on suspectedly infected hosts on the network in later investigations.

Further investigation of the malicious file

To further analyze any binary that was triggered by the YARA rule, the executable should be run in a sandbox environment. The following indicators of compromise can then be used to identify the file as either **Phobos** or **Blacksuit** ransomware:

1. Run the malicious file in a sandbox environment

2. Investigate if the file drops either of the depicted ransom notes in section 2.4

3. Investigate if the file adds the file extensions

id[-].[thekeyishere@cock.li].Elbie (**Phobos**)

.BlackSuit (**Blacksuit**)

to files

4. Investigate if the file performs any of the registry reads in table *registry keys* **in section 2.2**

5. Investigate if the file runs the command in section 2.2 in order to delete the shadow copies:

vssadmin.exe "*Delete Shadows /All /Quiet*" (Parent process: cmd.exe)

2.2 Identification of suspicious processes

If an endpoint has been infected with **Phobos** or **Blacksuit** ransomware and the file is allowed to run, the malicious process will perform actions that can be monitored for and responded to. If possible, the detection of the following actions combined with static features described above should cause the process to be killed. Before encryption, the

ransomware will perform system discovery and persistence tactics. Killing the process at this stage will prevent the ransomware from reaching the encryption phase.

2.2.1 Command line

Monitor for the following command line being run on a device:

- vssadmin.exe "*Delete Shadows /All /Quiet*" (Parent process: cmd.exe)

The command is used by both **Phobos** and **Blacksuit** to delete volume shadow copies, a snapshot of the computer's volume created by Windows as a security backup.

2.2.2 Suspicious registry reads

Registry key changes can be monitored on Windows using process monitoring and EDR systems. Before encrypting the files, the ransomware will use the following registry keys for system discovery. The keys contain information about the security settings on the device, allowing the ransomware to tailor its execution to the infected environment. An example of this is the system geolocation which tells the ransomware what language to display the ransom note in.

Registry key	Explanation
HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY RUNBINARYCONTROLHOSTPROCESSINSEPARATEAPPCONTAINER	This controls whether crucial internet explorer process runs in a secure, separated environment
HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ ACTIVECOMPUTERNAME	This contains the name of the computer
HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\INTERNET EXPLORER\SECURITY DISABLESECURITYSETTINGSCHECK	This setting controls whether the browser displays warnings to the user of insecure settings
HKLM\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\ CODEIDENTIFIERS TRANSPARENTENABLED	Controls to what files Windows' Software Restriction Policies (SRP) is applied
HKCU\CONTROL PANEL\INTERNATIONAL\GEO	This displays the geolocation of the computer
HKLM\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\ CODEIDENTIFIERS AUTHENTICODEENABLED	Controls that only signed executables are allowed to run, using SRP

Table 1 - Registry reads

If a process tries to access the following registry keys, it should be blocked and the parent file further investigated as specified in **section 2.1.**

The above registry keys hold information about the security settings on the system, including whether unsigned applications are allowed to run. Most legitimate software is signed by their vendor. Therefore, it is rarely necessary to disable these security settings that can be abused to allow the unsigned malware file to run.

Possible false positives include developer tools and software. These programs might edit the SRP to allow required DLLs to run.

2.3 Network anomalies indicating possible ransomware attack

If network traffic is monitored from a network tap, router or firewall, certain anomalies can indicate infection with ransomware.

The infected host will send broadcast requests using the deprecated NetBIOS protocol. The protocol is used for name resolution and file sharing on a local network. It has been replaced by more secure protocols in recent years, and the current recommendation is to disable the protocol unless critical legacy infrastructure depends on it. The ransomware will try to connect to devices on the local network by sending broadcasts with destination port 137. 137 is a special port for NetBIOS.

Be aware if the protocol is commonly used in the environment or not, and by which devices. Although this can be used for legitimate purposes, any anomalies/spikes in this behavior from a host should initiate further investigation according to the table of IOCs in **section 3**. The investigation should include a scan of the directories on the host with the YARA rule *phobosandblacksuit.yara* to detect malicious files. If the rule is triggered for a file, it should be investigated according to **section 2.1**.

If **Phobos** ransomware is present on a device in the network, the infected device will send repeated DNS and HTTP requests to the domain *ddos[.]dnsnb8[.]net* and IP *44.221.84[.]105*. Any contact with this domain should also be monitored for. If a host tries to connect, it should be isolated and investigated for the presence of suspicious files.

If **Blacksuit** has infected the device, it will send requests over SMB to port 445 systematically to all devices on the network to perform lateral movement and infect nearby devices. Anomalies or spikes in the use of this protocol should be monitored on the network and any findings lead to further investigation of the host sending out the requests.

2.4 Ransomware detected by encrypted device

If a machine has already been encrypted with ransomware, one of the following Ransom notes will be present on the system.

2.4.1 Phobos ransomware IOCs

- The presence of encrypted files with the file extension id[-].[thekeyishere@cock.li].Elbie
- The presence of the ransom note depicted in figure 4 in .hta format can be used to determine that it is **Phobos** type ransomware that has infected the machine.

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail thekeyishere@cock.li
Write this ID in the title of your message 9D6C40C2-3368
In case of no answer in 24 hours write us to this e-mail: recoverydata@onionmail.org
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 4 - Picture of the ransom note displayed on machines infected with Phobos ransomware

2.4.2 Blacksuit ransomware IOCs

- The presence of encrypted files with the .BlackSuit file extension
- The presence of the depicted ransom note in a .txt format is evidence that **Blacksuit** ransomware has infected the host.

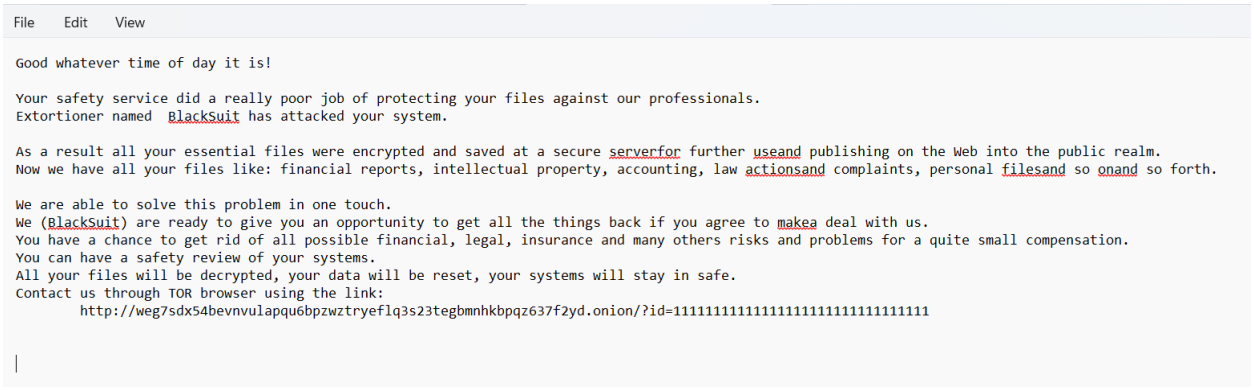

Figure 5 - Picture of the ransom note displayed on machines infected with Blacksuit ransomware

In figure 5, the id is equal to "1111.." This will however be unique for each victim.

To search for either of the ransom notes, perform a string search for the string

- ".onion"

to find the reference to the .onion mail address. The string search can be performed in a memory dump from the infected host, or by scanning the files on the device.

3. Containment

As the ransomware is able to successfully encrypt the device even without network connection, isolating the host device will not stop encryption from happening on the infected host. Isolating the device will however be crucial in preventing lateral movement. The ransomware will attempt to spread across the local network to other devices, including potential backup servers.

The first action in containment is to isolate the infected device from the local network to prevent lateral movement.

All hosts on the same local network as the infected device should be checked for the following IOCs of ransomware.

IOC	Where and how to search
phobosandblacksuit.yara **yararulehash.yara - containing the hash value identified in step 2, section 2.1**	All files on the system Email attachments Downloads
DNS requests to ddos[.]dnsnb8[.]net	Syslog/device timeline
Integrity check of STARTUP registry key	Regedit.exe
Verify shadow copies not deleted	Run the following command line to list all shadow copies on the system: vssadmin list shadows [/for=<ForVolumeSpec>] [/shadow=<ShadowID>]
Presence of encrypted files	Look for files with the following file extension: -id[-].[thekeyishere@cock.li].Elbie -BlackSuit.txt
Presence of ransom note	String search for ".onion" for the reference to the .onion email address in the notes. The search can be performed on directories, files, or in memory dumps. Search the filesystem for files with the name -Readme.BlackSuit.txt -info.hta

Table 2 - IOCs and relevant search methods

If any of the IOCs listed are detected on a device, it is considered infected and must be isolated for containing the incident.

While the infected devices are being taken out of operation, the backup system for business continuity which should have been implemented in phase 1 can be used in the meantime to enable normal operations. Backup services or solutions able to handle the critical services for the business will allow for business continuity and lower the impact of the original system being down.

4. Eradication

When the extent of the attack has been determined and all infected hosts identified, the threat must be removed from the environment. The eradication phase will depend on whether the ransomware did execute or not, and the initial infection vector used by the ransomware.

4.1 Encrypted devices:

Devices where the ransomware successfully encrypted files need to be re-imaged.

4.2 Non-encrypted infected devices

If the ransomware executable is present on the device but has not run or run unsuccessfully, the malicious file must be deleted. The device should be scanned with the rule *yararulehash.yara* containing the hash of the ransomware file used in the attack, to ensure no copies of the malicious file are hiding elsewhere on the system.

The YARA rule can be used to scan directories. It should also scan eventual email attachments. This is relevant as the ransomware has been observed being delivered by phishing emails.

4.3 Prevent reinfection according to the initial infection vector

Several methods for initial infection have been observed by the ransomware families. Depending on how it got onto the system, the following security measures should be implemented to ensure the attacker loses access to the system and to prevent reinfection.

4.3.1 Phishing email

Block sender of the email. Search for emails from the sender in the inbox of other accounts in the enterprise and delete all instances of this. Ensure the user has not interacted with the sender or provided credentials to eventual links. If credentials are revealed, perform steps in **section 4.3.3.**

4.3.2 Software vulnerability

This needs to be identified and patched according to software vendor recommendations. It is important that all devices are updated regularly.

4.3.3 Stolen credentials

If legitimate credentials have been stolen or compromised and used to get access to the device or system, the account needs to be disabled temporarily. It can be done by disabling it directly, or by resetting the password and revoking all active sessions. As the extent of the compromised credentials might go beyond the ransomware attack, the actions taken by the attacker with the compromised account must be investigated and remediated.

5. Recovery

Before the devices are either returned to use, they need to be ensured free from ransomware. Encrypted devices need to be re-imaged. The backups of eventual lost files created in the preparation phase can be reinstalled on the devices once they are ensured clean.

It is important to implement countermeasures to prevent the identified initial infection vector from being exploited again. Because the ransomware tries to read confidential information in the background to steal credentials, assuming that local accounts and locally stored credentials are compromised on the hosts where the ransomware was allowed to execute. After eradication, make sure the local credentials as well as email credentials used on the device are reset with a new password.

If the ransomware was delivered by email, the sender of the email must be blocked. If someone has clicked on a phishing link or email, they must change their password as it might have been compromised and could be used in attacks in the future. MFA should be enforced as best practice.

Any compromised RDP or similar accounts must change password before they are enabled again. Close the port on devices that do not need to use the remote connection protocol.

If unpatched software led to the malicious file being downloaded and executed, this must be addressed. If a patch has been released, ensure all systems install the patch. If this is not possible, consider stop using the software altogether or using a safer alternative such as a different vendor.

The systems and devices should be monitored on a regular basis for the IOCs used in this playbook. This should be implemented as EDR detection rules, network anomalies, log sources alerts or similar. Emails and downloads should be scanned for malicious files using antivirus software which blocks potentially malicious downloads automatically according to these IOCs.

As phishing emails and malicious links is a popular initial infection vector used in the described ransomware attacks, user training can help prevent ransomware attacks. User awareness and training can help prevent both credential theft through phishing as well as the user unknowingly downloading malicious files.

Acceptable Usage Policies can control whether a user is allowed to use their job credentials such as email and password for other webpages than what is required for work. Limiting this can help prevent the credentials from being leaked. Phishing simulation training can help prevent employees from interacting with phishing emails and malicious websites.

6. Lessons learned

The incident response process needs to be documented with analysis notes, overview of infected hosts, initial infection vector, and new IOCs detected.

It is important that the incident response process itself is documented and reviewed. Special attention should be given to what worked well in practice, and what unexpected problems did arise that were not addressed in the response plan beforehand. The plan should then be edited to address the problems to make the incident response more effective.

The documentation of a certain **Phobos** or **Blacksuit** incident might reveal new IOCs. The new malware samples obtained can be analyzed using the Hybridized-Comparative framework adapted for online sandboxes and used to develop new and more efficient detection rules. The findings can be used to further discover the development, similarities, and differences between new and old samples of **Phobos** and **Blacksuit** ransomware.

Glossary

Brute-force	The attacker cracks the password by systematically entering possible character combinations
C2	Command-and-control. Attacker controlled infrastructure used to communicate with the infected machine
Cryptocurrency	Digital valuta
Decryption key	A cryptographic key used to restore encrypted files
DLL	Dynamically linked libraries contain functions used by a program
EDR	Endpoint Detection and Response
Encryption key	A cryptographic key used to encrypt files to obscure the content
Entropy	A number indicating the randomness of the characters in a file
False positive	Detection incorrectly concluding with the occurrence of an incident
IDE	integrated development environment.
initial access broker	Cyber-criminals obtaining credentials and selling them to other cyber-criminals as an own business
IOC	Indicators of compromise. Evidence or artefacts on a system indicating the threat
NetBIOS	Deprecated protocol used for file sharing on a local network
Phishing email	Email designed to lure the victim into providing personal information to an attacker
RaaS	Ransomware-as-a-Service. Ransomware sold on the dark web to cyber criminals, enabling them to perform ransomware attacks even with limited technical competence.
RDP	Remote Desktop Protocol. Microsoft protocol used to connect remotely to a computer
Registry	Database structure in Windows containing the computer's current settings
Sandbox	An isolated computer environment typically used to safely run malware on
SHA256 sum	A string of characters unique to a file calculated based on its content
Shadow copies	Backups created automatically by Windows in forms of snapshots of the computer's volume
SMB	Service Message Block. A network file sharing protocol.
Social engineering	Interacting with the victim directly to trick them into revealing personal information or performing actions unknowingly
YARA	Yet-Another-Recursive-Acronym. A versatile language for writing malware detection rules

References

Cybersecurity & Infrastructure Security Agency. (2024). *#StopRansomware: Blacksuit (Royal) Ransomware* [Accessed 19-11-2024]. https://www.cisa.gov/newsevents/cybersecurity-advisories/aa23-061a

Kral, Patrick. (2011). Incident Handler's Handbook. (Whitepaper). SANS Institute. https://www.sans.org/white-papers/33901/

National Cyber Security Centre. (2024). Glossary [Accessed 19-10-2024].www.ncsc.gov.uk. https://www.ncsc.gov.uk/section/advice-guidance/glossary

NCCoE. (2023*). PROTECTING DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS*. National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-dataextended.pdf

Schmitt, V. (2019). *A comparative study of CERBER, MAKTUB and LOCKY Ransomware using a Hybridised-Malware Analysis Framework* [Submitted in Partial fulfilment of the Requirements of the Degree of Master of Science at Rhodes University]. Rhodes University [Identifier: http://hdl.handle.net/10962/92313].