[CLIENT] [DATE]
Ransomware Simulation Report

Date / Version

Project Objective

Abacus Group was contracted to perform breach simulation testing in the form of Tabletop Testing of Ransomware Attacks on System Backups and Technical Ransomware Attack Simulation on Internal Systems between the dates of [DATE], and [DATE], on [CLIENT]. The integration of both tabletop and technical analysis enabled Abacus Group to accurately assess the viability of internal policies, procedures, and security controls and identify security control gaps as applicable. Additionally, scenarios designed by Abacus Group emulated a real-world advanced persistent threat (ATP) of moderate sophistication whose intent was to compromise [CLIENT] using ransomware.

Objectives of this Exercise:

- **Abacus Group will review and evaluate the backup systems, including the overall architecture, utilized software, configurations, and security safeguards.**
- **Abacus Group will evaluate if backup reports, configurations, and safeguards adhere to organization policies and procedures.**
- **Abacus Group will identify security weaknesses in the backup architecture and configurations that can be exploited by ransomware attacks and lead to backup data being deleted.**
- **If necessary, Abacus Group will provide recommendations on improving the backup architecture in practical ways to reduce the chances of a ransomware attack leading to backup data being deleted.**
- **Abacus Group will conduct an in-depth technical analysis of [CLIENT] internal network architecture to validate the presence of security controls objectively.**
- **Abacus Group will evaluate the results of the ransomware simulations to identify areas of improvement that will reduce the attack surface of [CIENT] systems.**

Abacus Group's analysis and recommendations are in accordance with the guidelines outlined in NIST SP 1800-11 (Data Integrity: Recovering from Ransomware and Other Destructive Events), NIST SP 1800-25 (Identifying and Protecting Assets Against Ransomware and Other Destructive Events), and NIST SP 1800-26 (Detecting and Responding to Ransomware and Other Destructive Events).

Project Points of Contact at [CLIENT]

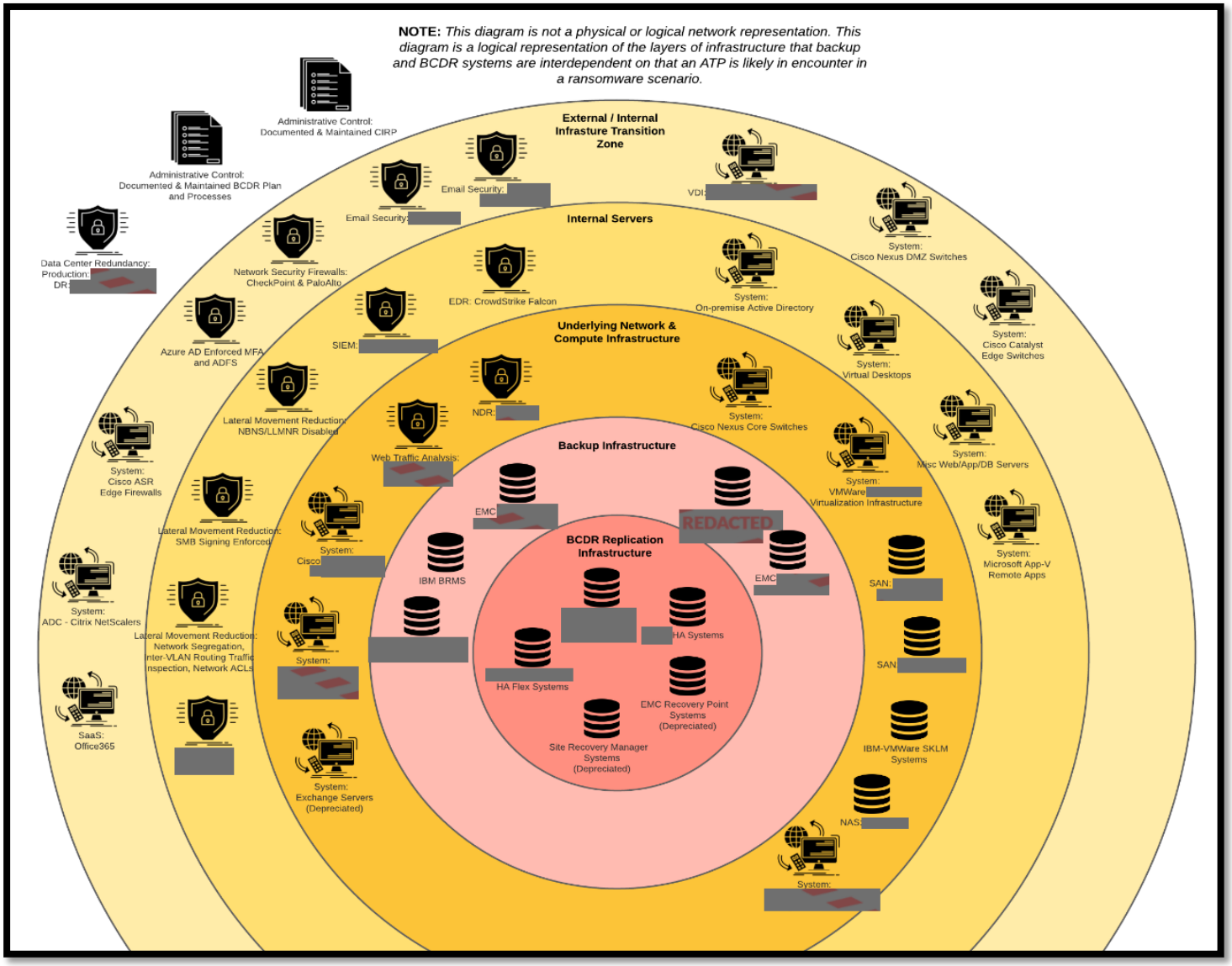
Full Name	Title	Email Address
REDACTED (Primary Point of Contact)	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED

Provided Documentation

Item #	Data Source Name	Source Type
1	REDACTED	.docx
2	REDACTED	.pdf
3	REDACTED	.docx
4	REDACTED	.docx
5	REDACTED	.xlsx
6	REDACTED	.docx
7	REDACTED	.docx
8	REDACTED	.docx
9	REDACTED	.pptx
10	REDACTED	.pdf
11	REDACTED	.docx
12	REDACTED	.docx
13	REDACTED	.docx
14	REDACTED	.pdf
15	REDACTED	.docx
16	REDACTED	.docx
17	REDACTED	.docx
18	REDACTED	.xlsx
19	REDACTED	.doc

Project Methodology

For this project, [CLIENT]'s objective was to verify that robust security controls are implemented across their information systems that prevent backups from being tampered with by malicious actors. In order to properly assess this, Abacus Group designed a tailored four-phase methodology. During the first phase, Abacus Group engineers analyzed the nineteen documents provided by [CLIENT] (see section 1.2) in order to determine currently enforced policies and procedures. Abacus Group also reviewed and evaluated the backup systems in place, including the overall architecture, utilized software, configurations, SMB file share permissions, and organization security safeguards. Further clarification was provided by the project point of contact(s) (see section 1.1). The following diagram represents a visualization of those security controls in a logical design.

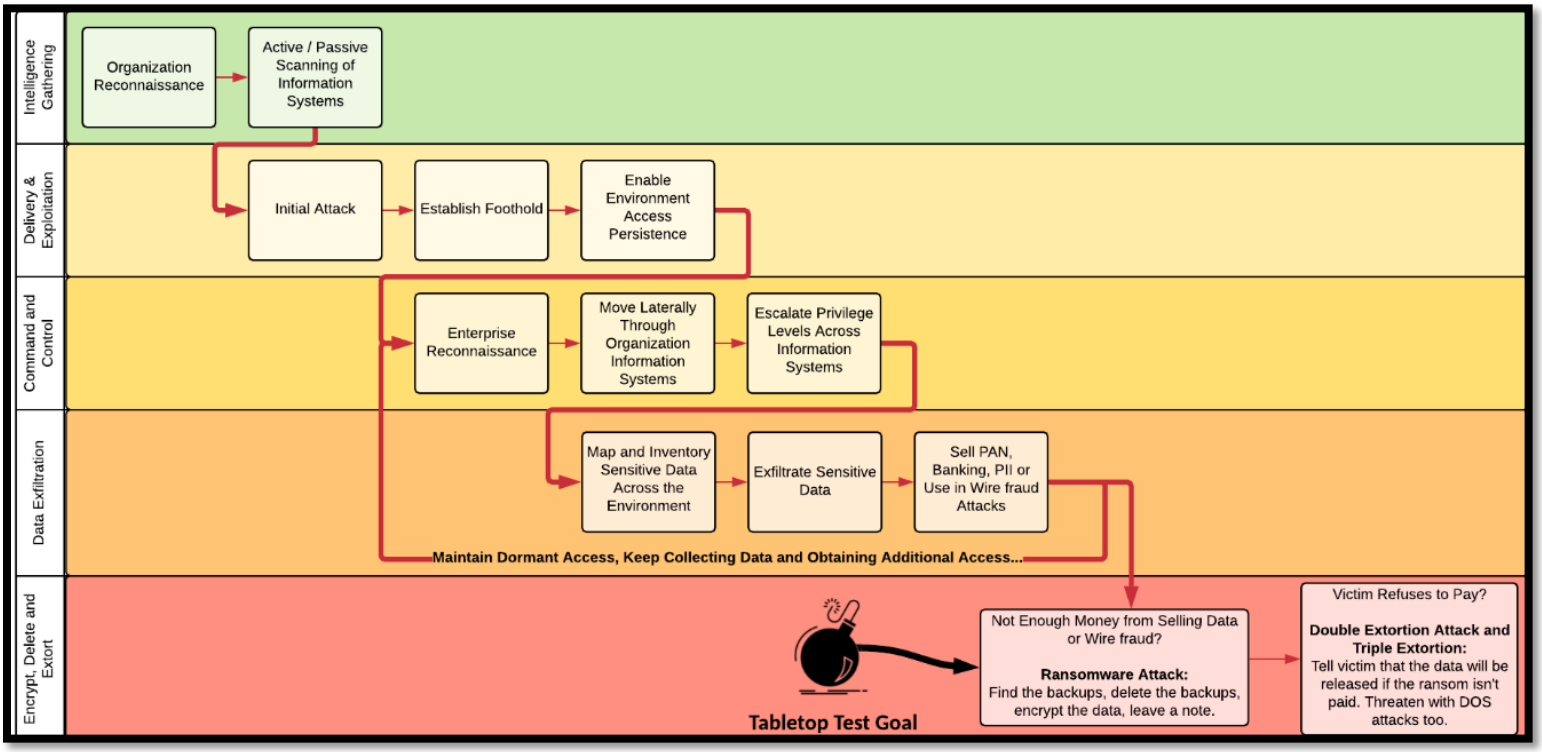


Based on this understanding, Abacus Group was able to move to the second phase of the operation. During this phase, Abacus Group identified weaknesses in the backup architecture and configurations that could be exploited by ransomware attacks which could lead to backup data being deleted.

Abacus Group determined four distinct attack scenarios used by malicious actors of varying skill and resource levels. Scenarios ranged from a malicious actor of a low technical capacity to state-sponsored advanced persistent threats (APTs).

Scenario	Initial Attack Vector	Type of Attacker	Likeliness
1	Social Engineering	Script Kiddie – Moderately Sophisticated APT	High
2	SQL Injection	Small APT – Moderately Sophisticated APT	Moderate
3	Zero-Day Vulnerability	Moderately Sophisticated APT - State-Sponsored APT	Low
4	Attack on Supply Chain	State-Sponsored APT	Low

Notably, in the above chart, as the technical capacity required for an attack increases, the likeliness of [CLIENT] to be targeted by such an attack vector decreases. These attack vectors are in line with the currently available industry data. Each scenario followed an attack methodology utilized by malicious actors beginning with organizational reconnaissance, establishing a foothold and gaining persistence, moving laterally in the environment, escalating privileges, exfiltrating sensitive data, compromising backups, and launching a ransomware attack. This process is illustrated below.

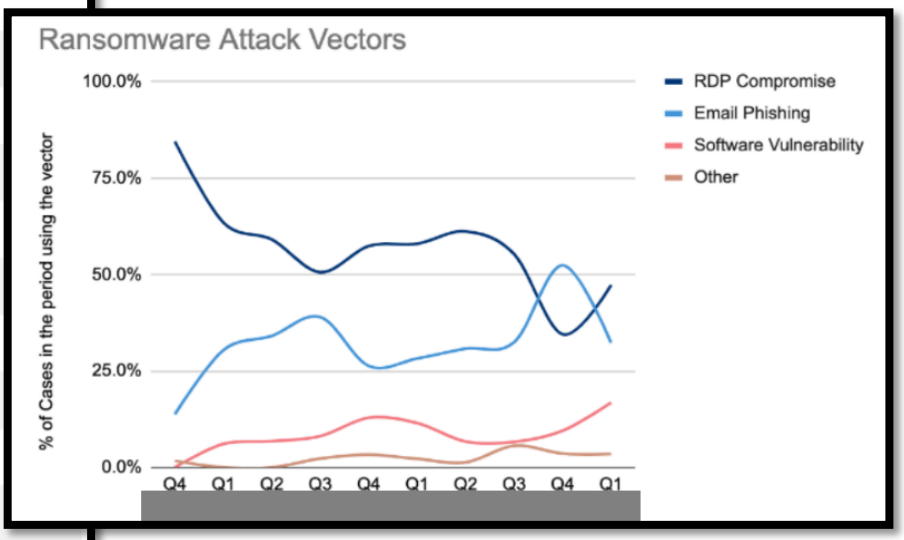


These four scenarios were outlined by Abacus Group in graphical representations and discussed with the [CLIENT] team during two separate one-hour tabletop testing sessions. The tabletop sessions allowed stakeholders to understand the kill chain of these popular attack vectors and identify each point with which [CLIENT] security controls were implemented.

During each of these scenarios, Abacus Group assigned numerical probabilities of success for each element of the attack vector from the standpoint of the APT. These statistical values represent estimates based on up-to-date industry data regarding cybersecurity threats, the level of maturity of [CLIENT]'s security posture, and internal expertise built through years of red teaming engagements.

To further supplement the insight gained during the tabletop exercises, Abacus Group transitioned to phase three, technical evidence collection. The primary tools utilized during this phase were Wireshark and Network Detective. Wireshark is a network traffic analyzer, which can capture and analyze packets on the network. Network Detective is an IT managed service provider (IT MSP) tool that is used to perform discovery in Active Directory environments. [CLIENT] provided Abacus Group with VDI access in order to facilitate this white box testing. The technical evidence collected during this phase was used to confirm the presence of security controls discussed during the tabletop scenarios, map SMB file share permissions and identify any additional avenues of attack that were not initially identified from phase one. The fourth and final phase of the operation involved a collective analysis of the aggregate information from all other phases and report production.

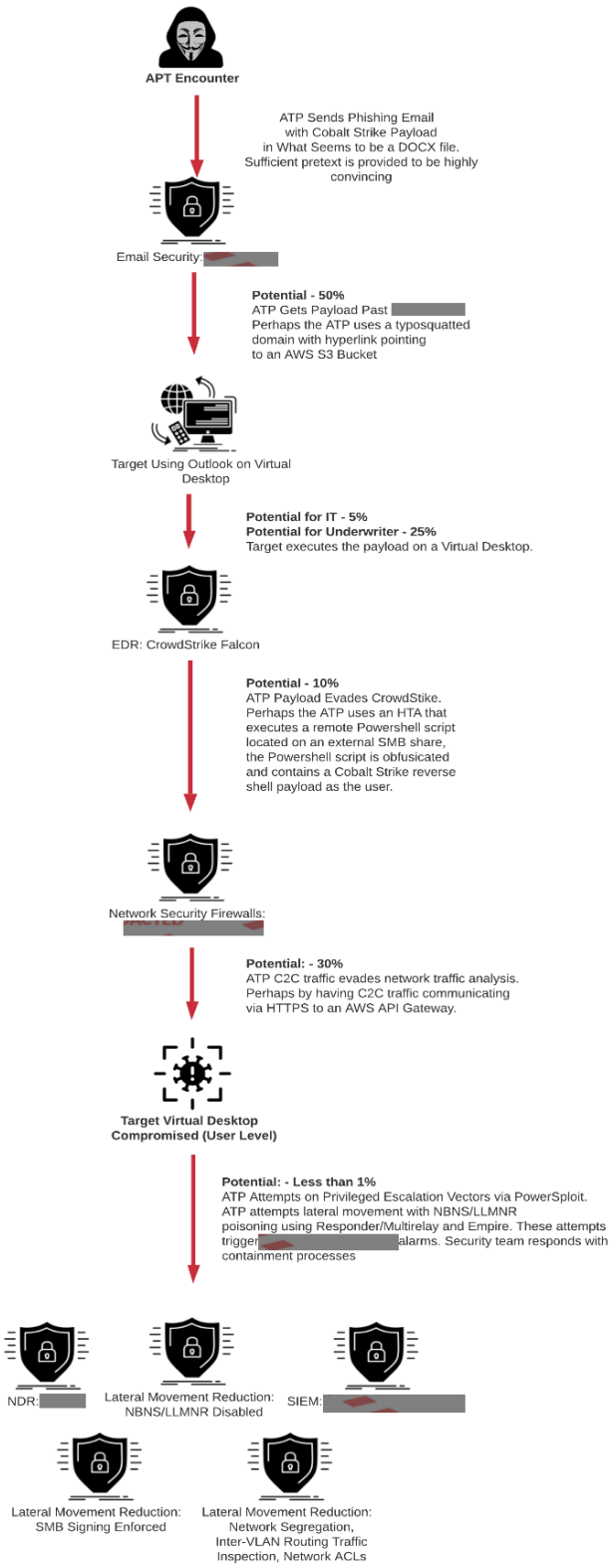
Rank	Ransomware Type	Market Share %
1	Sodinokibi (REvil)	14.2%
2	Conti V2	10.2%
3	Lockbit	7.5%
4	Clop	7.1%
5	Egregor	5.3%
6	Avaddon	4.4%
7	Ryuk	4.0%
8	Darkside	3.5%
9	Suncrypt	3.1%
9	Netwalker	3.1%
10	Phobos	2.7%



Tabletop Testing of Ransomware Attack on System Backups

Scenario 1

The first scenario analyzed during tabletop testing involved a malicious actor targeting either an underwriter or a member of the IT staff through social engineering. Specifically, using a phishing email with an embedded payload is a very common attack vector used by malicious actors to gain an initial foothold into the network. Due to the widespread knowledge of this attack and the availability of tools designed to accomplish it, Abacus Group assessed the likelihood that [CLIENT] could be targeted in this way as high. Furthermore, this attack may be performed by very rudimentary hackers, also known as script kiddies, as well as advanced persistent threats (APTs).



The attacker would begin with social engineering. Perhaps reaching out to an underwriter as a potential customer or impersonating an employee through a typo-squatted domain and reaching out to IT personnel. Sufficient pretext would be built up before the attacker sends an email with a malicious payload disguised as a DOCX file. Through an analysis of documentation and technologies used by [CLIENT], Abacus Group assessed a 50% chance the malicious payload could bypass the Mimecast email management software. Assuming the email did reach an end-user, the security awareness of those individuals would determine if the DOCX was executed, ignored, or reported. [CLIENT] provided documentation indicating that annual security awareness training for employees is a currently enforced policy. Abacus Group assessed a 5% chance of IT personnel and a 20% chance of an underwriter executing the payload.

[CLIENT] utilizes CrowdStrike Falcon as a cloud-based Security as a Service (SaaS) solution. Abacus Group assessed only a 10% chance that an attacker would successfully evade CrowdStrike Falcon with the payload. In the event the attack was successful, the attacker may utilize an HTA to remotely execute a PowerShell script located on an external SMB share. The PowerShell script would be obfuscated and contain a Cobalt Strike reverse shell payload. The attacker would then be forced to contend with

network security firewalls that [CLIENT] utilizes. Assuming the attacker is using an AWS API gateway to send command and control communications over HTTPS, Abacus Group assessed a 30% chance of evading network traffic analysis.

At this point, the attacker would have compromised an end-user's workstation. The next logical step would be for the attacker to attempt to escalate their privileges. The most likely method of this would be using PowerSploit while simultaneously attempting lateral movement via NBNS/LLMNR poisoning through the use of tools such as Responder and Empire. However, both NBNS and LLMNR are disabled by [CLIENT], and SMB signing is enforced. Supporting technical evidence related to NBNS, LLMNR and SMB may be found in section 3 (Technical Data Collection and Analysis). Lateral movement is further reduced as [CLIENT] has implemented network segmentation, inter-VLAN routing traffic analysis, and network ACLs. These safeguards which are implemented would significantly diminish the likelihood of success for an attacker using this attack vector. Furthermore, these attempts would trigger ` as well as REDACTED alarms, at which point the [CLIENT] security team would respond with their containment process. The aggregate of these safeguards reduced the likelihood of an attacker successfully escalating their privileges to less than 1%.

This scenario analyzed one of the most common attack vectors used by malicious actors in compromising organizations of similar size to [CLIENT]. The robust defense in depth strategy utilized by [CLIENT] will make it very unlikely that this attack vector would prove to be viable to an attacker. Abacus Group assessed [CLIENT]'s vulnerability to the attack vectors utilized in this scenario as Low.

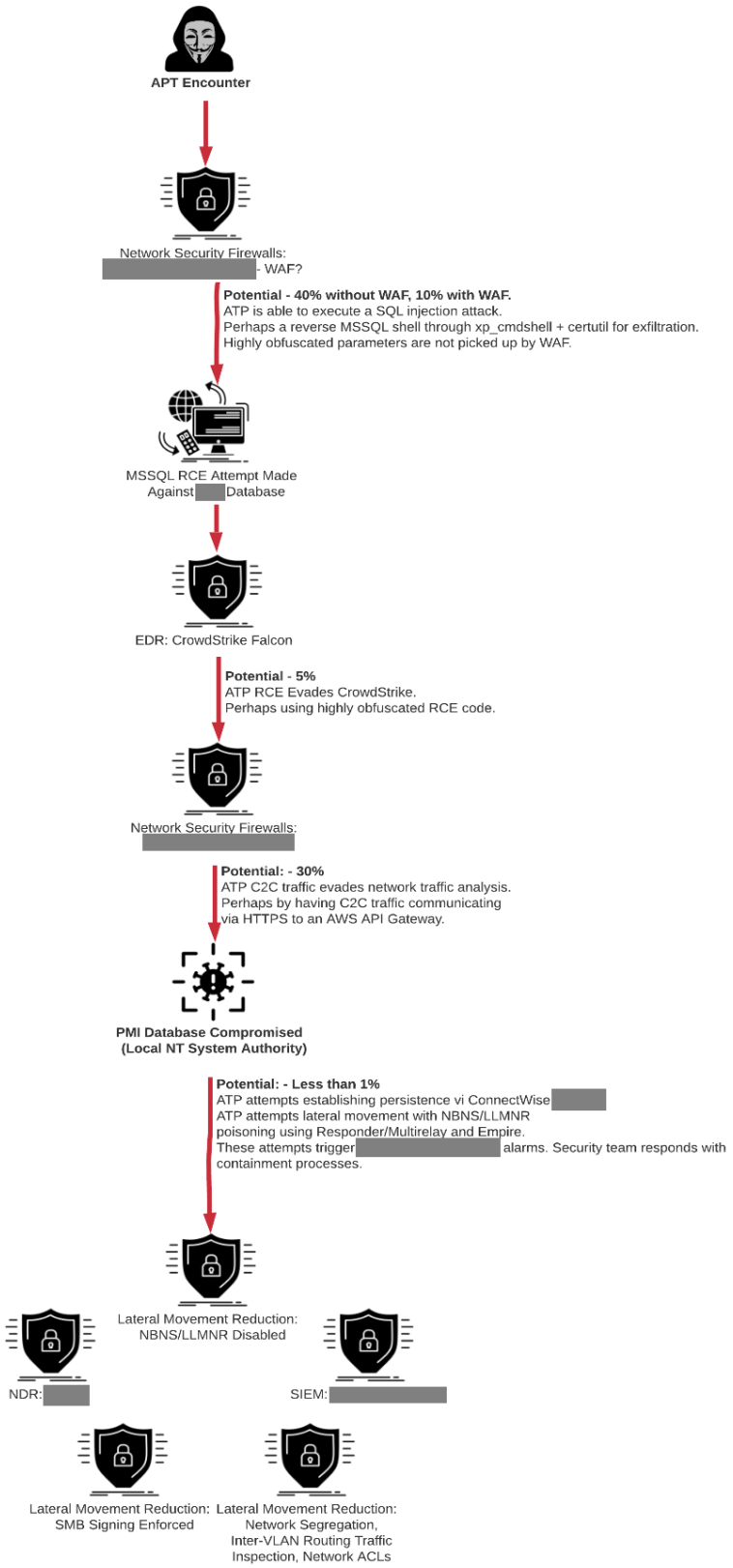
Scenario 2

The next scenario analyzed through tabletop testing involved an attacker executing an SQL injection attack on the [CLIENT]web application. SQL injection involves an attacker manipulating an interpreter into executing unintended commands. The Open Web Application Security Project (OWASP) lists injection attacks as #1 in its widely referenced Top Ten list of the most critical risks to web applications. This attack vector would be utilized by a more sophisticated APT than as described in Scenario 1. Abacus Group assessed a moderate likelihood that [CLIENT] would be attacked in the following manner.

An ATP would need to compromise a user account in order to begin this attack vector, as the SQL injection would require authenticated access.

The first obstacle for the APT lies in network security firewalls implemented by [CLIENT]. After analyzing documentation related to REDACTED, Generally. Web Application Firewalls (WAFs) are useful in reducing the chances of a successful SQL injection attack but are not perfect. A moderately skilled APT would likely highly obfuscate parameters in order to bypass a WAF. For this reason, there is a degree of residual risk that remains even with a WAF correctly implemented. The APT's injection attack could potentially utilize a reverse MSSQL for exfiltration. Remote code execution attempted against the [CLIENT]database would likely be thwarted by CrowdStrike Falcon.

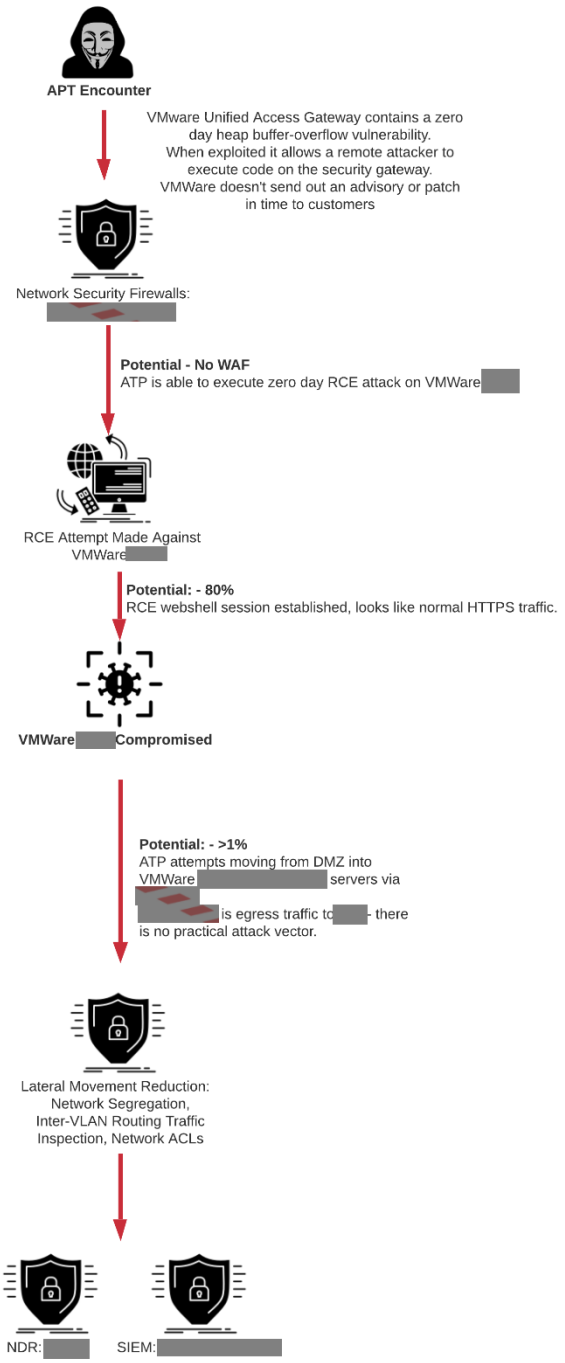
There remains the possibility that a highly skilled APT could obfuscate parameters to a sufficient degree that the RCE code could evade CrowdStrike Falon, but Abacus Group assessed that probability at only 5%. The APT would need to avoid network traffic analysis for command and control communication. One method that the APT may use would be communicating via HTTPS over an AWS API gateway. The likelihood of this communication going unnoticed by network analysis mechanisms was assed as 30%.



At this point, the [CLIENT]database would be compromised at the Local NT system authority level. The APT would then attempt to establish persistence, move laterally, and elevate their privileges. Persistence attempts may be established via ConnectWise. The lateral movement would likely be attempted through NBNS/LLMNR poisoning through the use of tools such as Responder and Empire. As seen in scenario 1, robust security controls to include NBNS and LLMNR being disabled, SMB signing being enforced, network segmentation, and network ACLs reduce the viability of this attack vector significantly. The attempts by the APT would trigger REDACTED and REDACTED alarms which would alert the [CLIENT] security team, and containment processes would begin. This scenario analyzed one of the most critical attack vectors used by malicious actors in compromising web applications of organizations similar in size to [CLIENT]. The robust defense in depth strategy utilized by [CLIENT] will make it very unlikely that this attack vector would prove to be viable to an attacker. Abacus Group assessed [CLIENT]'s vulnerability to the attack vectors utilized in this scenario as Low.

Scenario 3

The third scenario analyzed during a tabletop testing session involved an APT exploiting a zero-day vulnerability in VMWare REDACTED. A zero-day vulnerability refers to a security vulnerability that was previously unknown and, by extension, would be unpatched by the developer at the time of exploitation. This scenario assumes the malicious actor had the resources and technical capacity to identify and exploit a previously unknown heap buffer-overflow vulnerability. When a vulnerability of this nature is exploited, it will allow a remote attacker to execute code on the secured VMWare Unified Access Gateway.



As this scenario assumes it is a zero-day vulnerability, VMWare is not able to send out an advisory notice or software patch prior to [CLIENT] being targeted by an attacker.
There is a reasonable expectation that the APT would be able to execute a zero-day RCE attack on VMWare REDACTED despite [CLIENT]'s implemented Palo Alto network security firewall and intrusion prevention system (IPS).

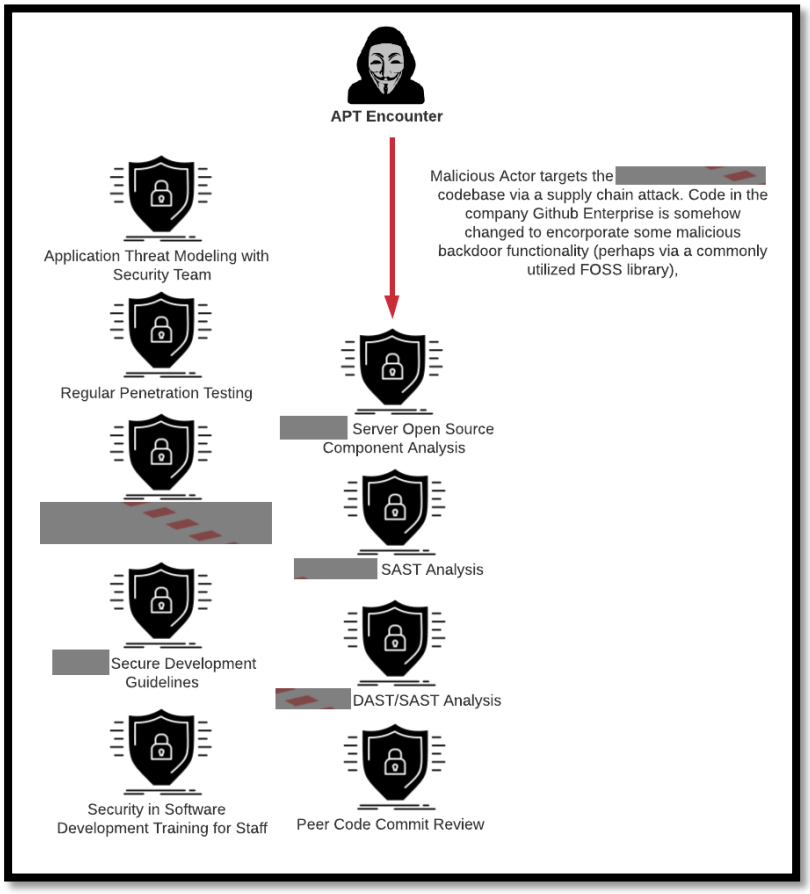
Following the compromise of the VMWare REDACTED, the APT would attempt to move from the demilitarized zone (DMZ) into VMWare Connection Servers via XML-API. The potential for this movement from a compromised VMWare REDACTED into the underlying VMWare environment is very low. For this to be a viable attack vector, there would need to be multiple zero-day vulnerabilities in multiple VMWare products that could be incorporated in tandem. VMWare is an entirely separate product and uses a different code base than VMWare REDACTED, which makes the likelihood of the same vulnerability being identified in both products extremely unlikely. For this reason, Abacus Group assessed a less than 1% chance of the APT being successful in lateral movement.

In the unlikely scenario that two high severity zero-day vulnerabilities resulted in an APT moving into the underlying VMWare environment, further attempts at lateral movement and privilege escalation would likely be prevented through the presence of robust security controls.

As seen in scenarios 1 and 2, security controls to include NBNS and LLMNR being disabled, SMB signing enforced, network segmentation, and network ACLs reduce the viability of this attack vector significantly. The attempts by the APT would trigger REDACTED and REDACTED alarms which would alert the [CLIENT] security team, and containment processes would begin. Abacus Group assessed [CLIENT]'s vulnerability to the attack vectors utilized in this scenario as Low.

Scenario 4

The last scenario was a different approach and focus than the previous ones. Scenario 4 was developed in real-time on an [CLIENT] tabletop testing meeting instead of the previous hybrid approach of developing scenario paths offline (not interactively on a meeting). Furthermore, Scenario 4 focused on a much different attack vector than the previous campaigns by simulating a supply chain attack situation.



Supply chain attacks on organizations and their underlying code repositories are becoming more and more frequent, as demonstrated with recent supply chain attacks against Codecov and the PHP development team.

This scenario assumed the most likely attack vector of a compromised free and open-source (FOSS) library such as OpenSSL, OpenSSH, etc.

[CLIENT]'s Connect Origination software is developed in-house and utilizes many FOSS libraries and components.

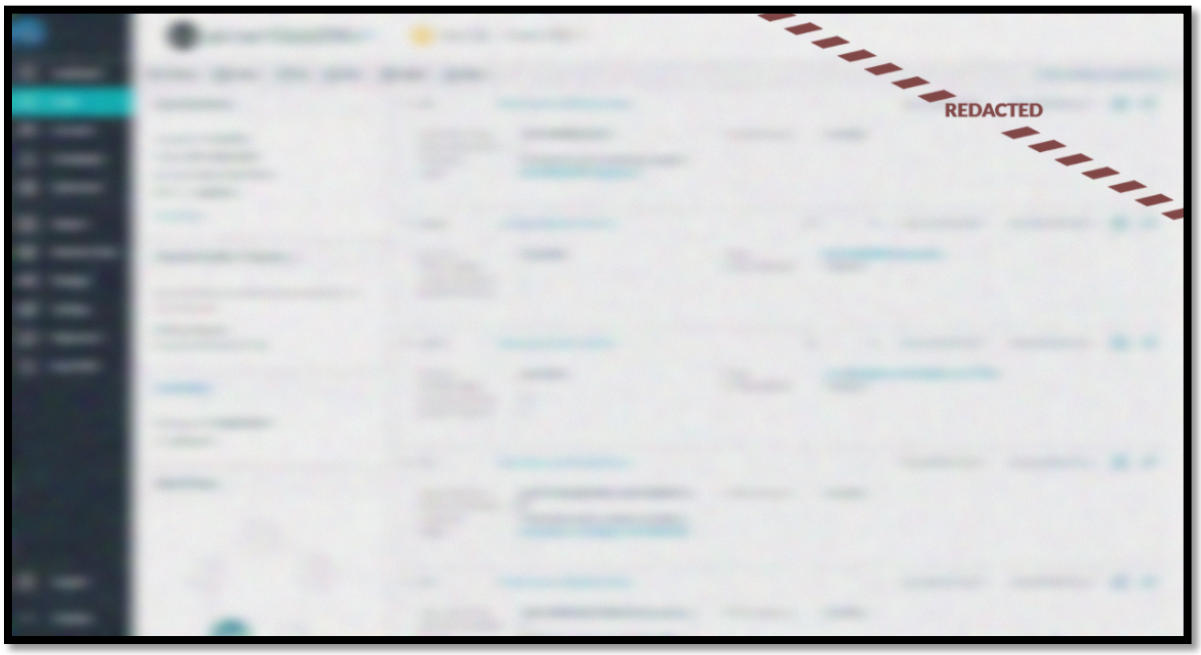
The scenario foothold was a situation where a malicious backdoor was injected into an underlying FOSS component utilized by [CLIENT]'s Connect Origination software. When discussing such an attack scenario with the [CLIENT] team, it became quite apparent that [CLIENT] has multiple overlapping security safeguards that help proactively detect malicious code introduced into the Connect Origination codebase prior to production deployment.

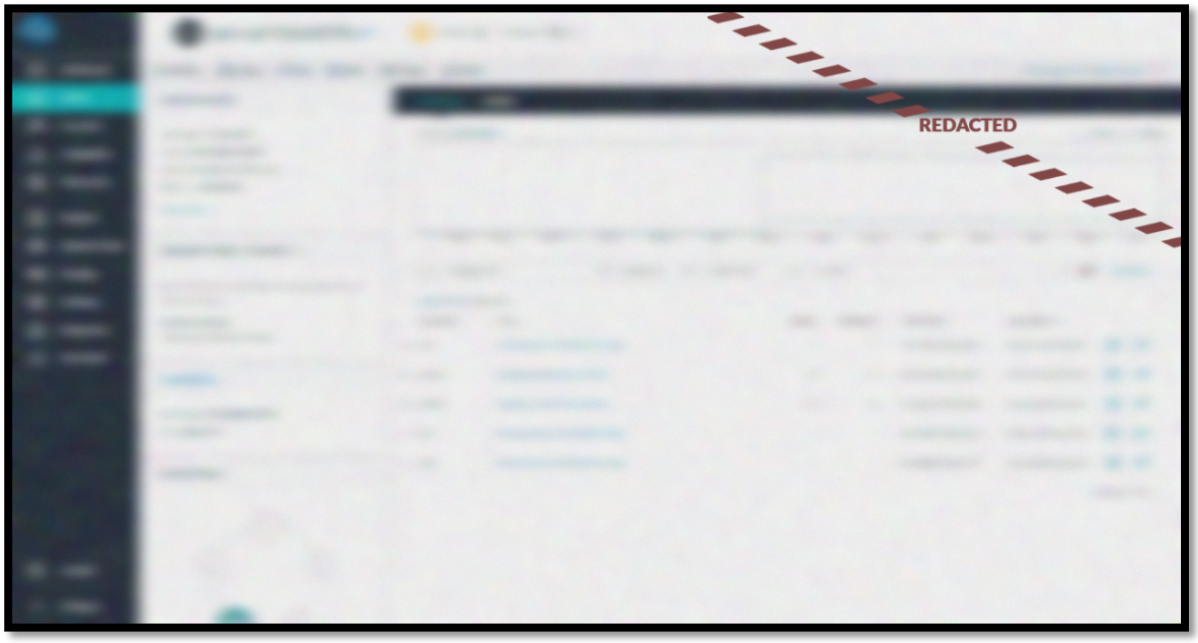
Most notably, REDACTED and REDACTED are utilized in dynamic application security testing and static application security testing, which would help detect malicious code introduced to the code repository via a compromised FOSS library. Furthermore, Nexus IQ is employed in [CLIENT]'s software development lifecycle to analyze and measure the risk level or various FOSS libraries utilized by the Connect Origination software. Lastly, [CLIENT]'s software development collaborates with the security team so that elements of a defense-in-depth approach are incorporated into the organization's software development lifecycle, such as secure development guidelines, application threat modeling, annual penetration testing, and more.

Completely avoiding a supply chain attack is unaccomplishable for any organization regardless of their cybersecurity maturity level; rather, that focus should be proactive detection, response, and containment of a supply chain attack before it has any ability to impact the organization. That said, Abacus Group observed robust, proactive security controls to effectively detect and mitigate such a supply chain attack, with the actual risk of this scenario being Low.

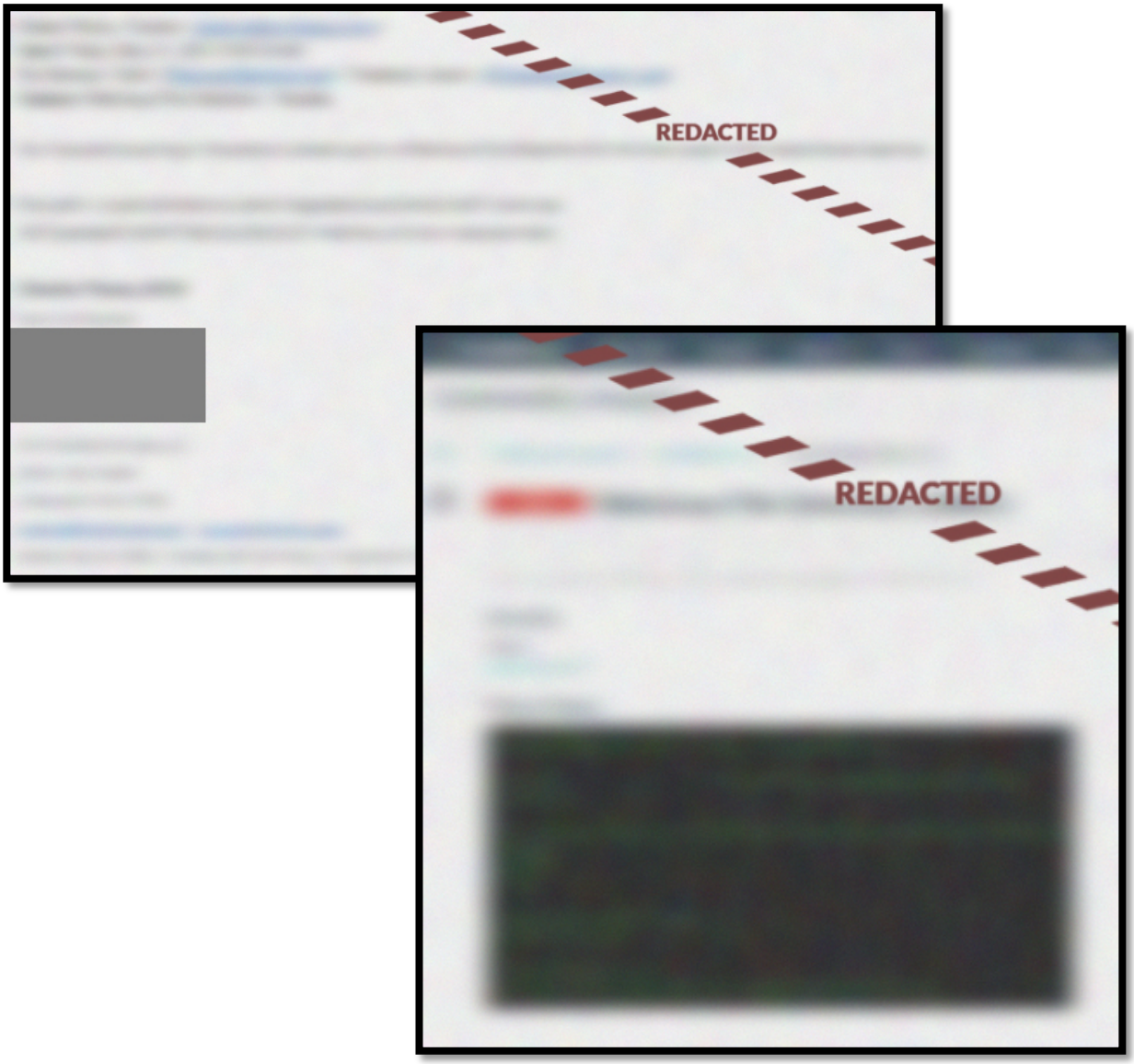
Technical Data Collection and Analysis

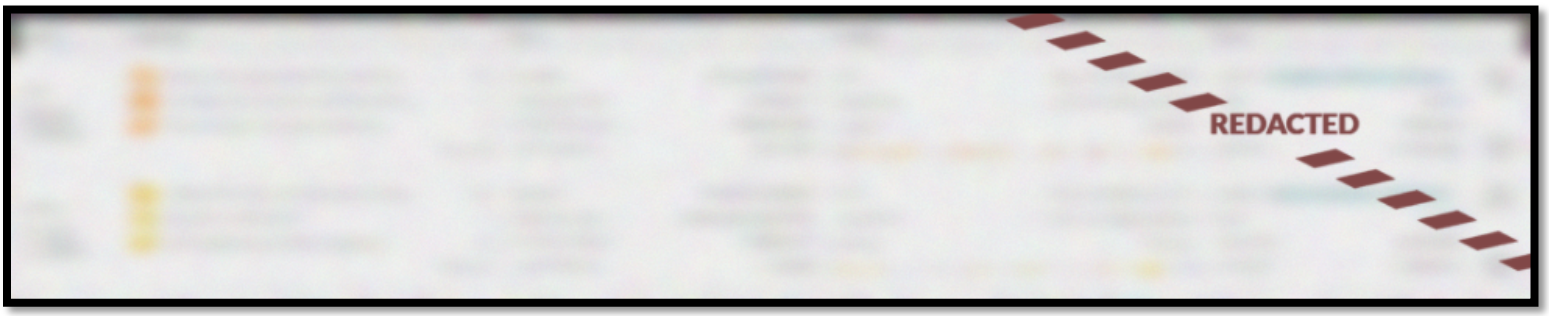
Abacus Group initiated technical evidence collection and analysis on [DATE] through the use of a VDI provisioned by [CLIENT]. For this effort to be successful, REDACTED had to white list Network Detective in order for the tool to function. [Date], Abacus Group was alerted by REDACTED with the [CLIENT] security team to confirm numerous notifications and alerts which were caused by Network Detective.



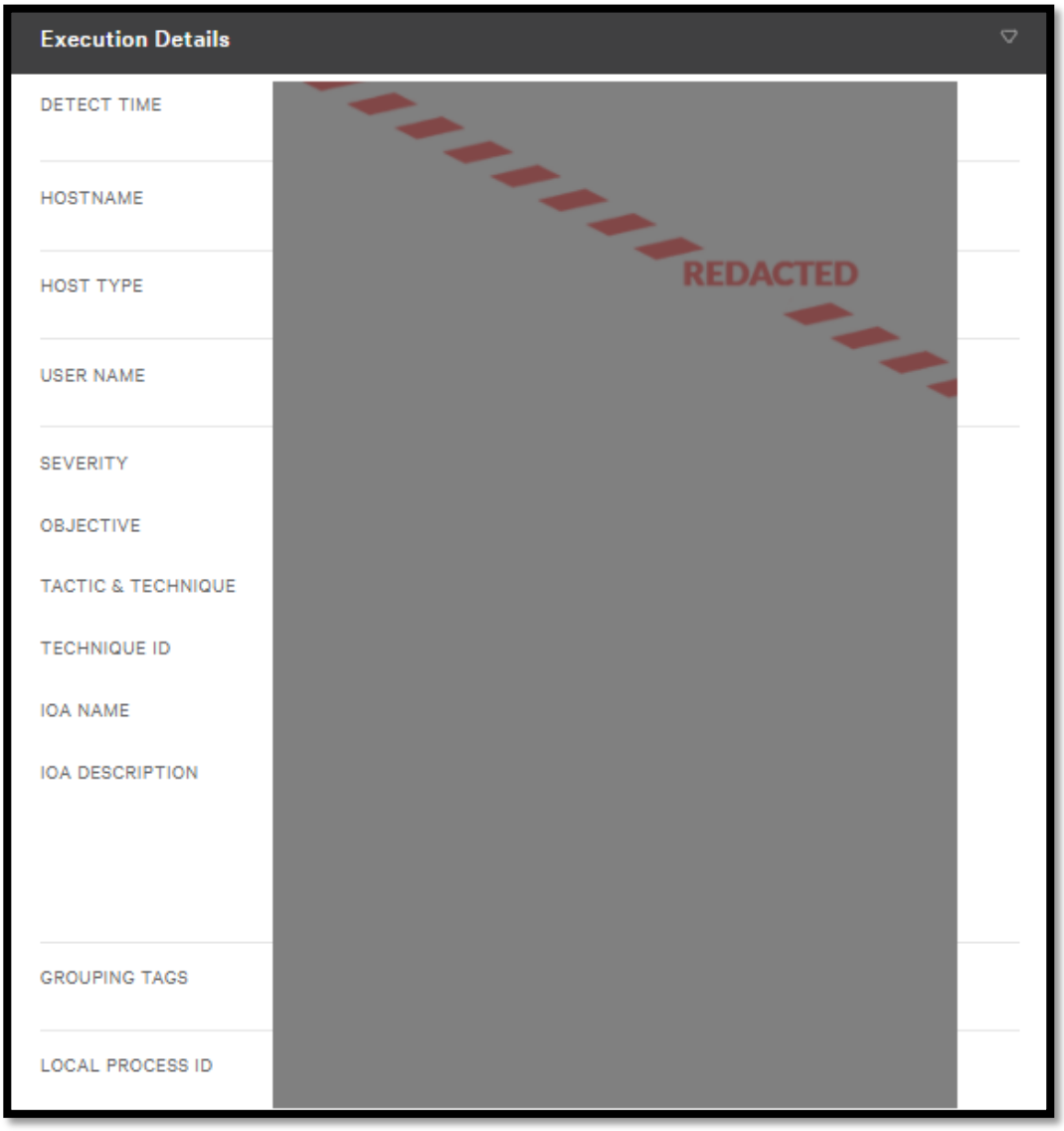


In addition to alerts generated by REDACTED and REDACTED, CrowdStrike also detected potentially malicious activity. While the alerts generated by CrowdStrike were not attributed to the simulation, it is significant that exceptions made to facilitate it did not impact CrowdStrike functionality. The system continued to monitor, detect, and alert. This evidence demonstrates that [CLIENT] has a mature Change/Release Management Process.



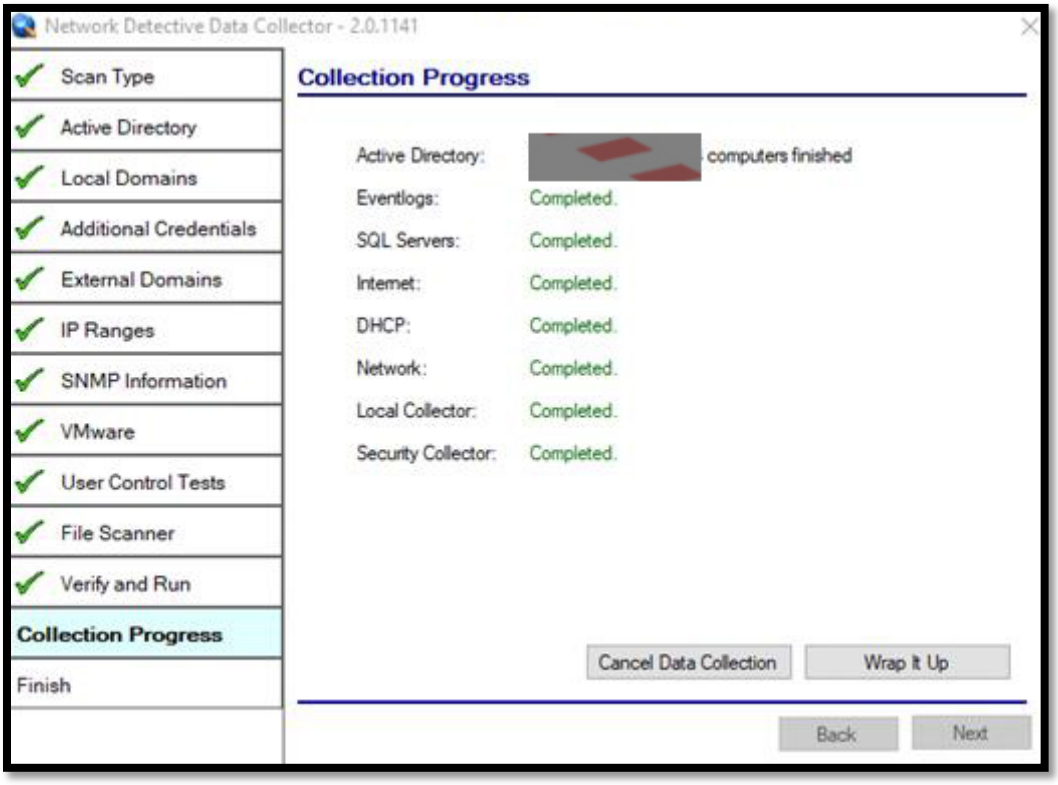


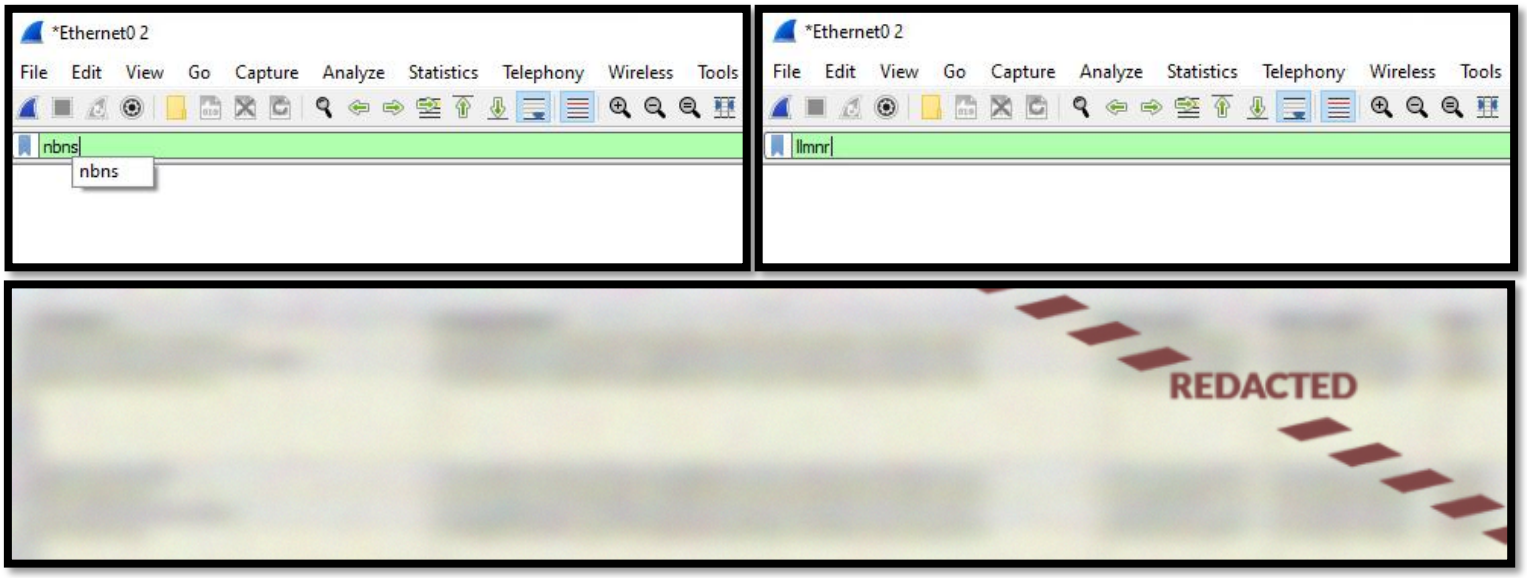

REDACTED


Execution Details
DETECT TIME
HOSTNAME
HOST TYPE
USER NAME
SEVERITY
OBJECTIVE
TACTIC & TECHNIQUE
TECHNIQUE ID
IOA NAME
IOA DESCRIPTION
GROUPING TAGS
LOCAL PROCESS ID
REDACTED

The Network Detector scan was conducted against all active directory connected systems, including all of the following subnets, which contain critical backup infrastructure.

IP	ACL	Environment	Function/Description	CIDR	Priority for Ransomware Scan
REDACTED	Yes	PRD	REDACTED	REDACTED	
REDACTED	Yes	PRD	REDACTED	REDACTED	
REDACTED	No	PRD	REDACTED	REDACTED	TRUE
REDACTED	No	PRD	REDACTED	REDACTED	TRUE
REDACTED	No	PRD	REDACTED	REDACTED	
REDACTED	No	PRD	REDACTED	REDACTED	TRUE
REDACTED	No	PRD	REDACTED	REDACTED	
REDACTED			REDACTED	REDACTED	TRUE
REDACTED			REDACTED	REDACTED	TRUE
REDACTED			REDACTED	REDACTED	TRUE





In addition to Network Detective, Wireshark was used to identify types of traffic on the network. Specifically, Abacus Group looked for the presence of NBNS and LLMNR traffic. Further analysis of Network Detective results shows that [CLIENT] had disabled NBNS and does enforce SMB signing.

[CLIENT] also has implemented group policy objects for hardening systems, demonstrating a robust security environment.

Based on these observations, it would be considerably difficult for a malicious actor to gain a foothold into [CLIENT] systems and laterally move fast enough to execute a full-scale cryptolocker ransomware attack (which would require the sabotage of backups and BCDR systems) without setting off security alarms.

That said, most high-profile ransomware attacks executed by ATPs like REvil, Conti, Darkside, and Ryuk involve double-extortion or triple-extortion attacks. More specifically, double-extortion and triple-extortion attacks go beyond cryptolocking important corporate files and employ exfiltration of confidential company data, threats of confidential data leakage, and threats of further attacks (sometimes involving DoS attacks).

In tandem with Network Detective, Abacus Group utilized an [CLIENT] provisioned user account (cscott) to validate the filesharing permissions of various company SMB file shares. A full set of

spreadsheets is included with this report. Still, Abacus Group observed what seemed to be a handful of file shares set with everyone READ permissions that may contain sensitive data that could be easily accessed and potentially exfiltrated by a malicious actor (if they could gain a foothold into a user account), including directories that contain various backups, logs, and QuickBooks data. Abacus Group did not read the contents of any file shares, so the accuracy of what is contained in these directories is up for question and will need to be verified further by [CLIENT]'s IT department and security team. Many of these file shares also grant WRITE permissions which could be used by cryptolocker malware to encrypt files and delete the original copies. Note that NTFS filesystem permissions couldn't be reliability be enumerated, which may change actual read/write abilities beyond SMB permissions.


REDACTED

Conclusion and Recommendations

[CLIENT] demonstrated a mostly mature security posture with robust technical controls objectively verified through technical analysis. Compiled risk results of the tabletop exercises aggregated with technical analysis can be seen in the table below.

Tabletop Testing of Ransomware Attack on System Backups Results			
Scenario	**Initial Attack Vector**	**Probability of Success (for an APT)**	**Risk to [CLIENT]**
1	Social Engineering	Low	Low
2	SQL Injection	Low	Low
3	Zero-Day Vulnerability	Low	Low
4	Attack on Supply Chain	Low	Low

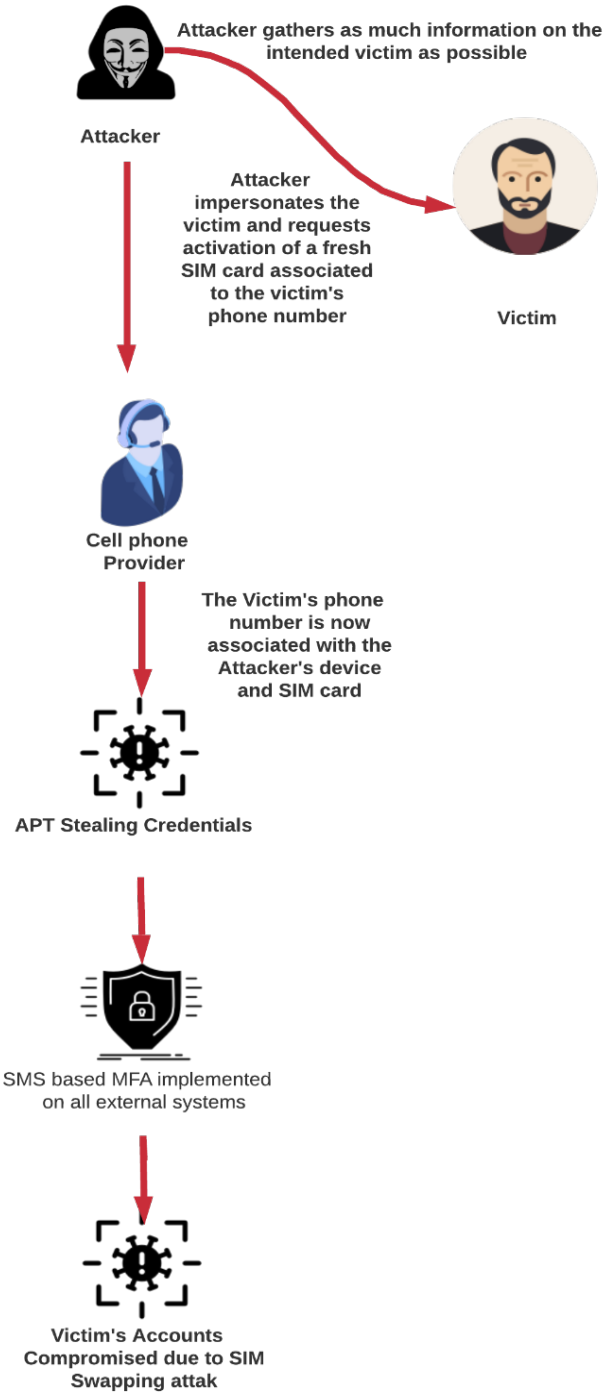
Based on observations made during both the technical analysis and tabletop exercises, Abacus Group engineers identified five distinct recommendations to further enhance [CLIENT]'s security posture. While most of these recommendations address a concern rated to be a low risk to [CLIENT], the combination of multiple vulnerabilities can increase the overall risk profile of an organization.

Top Recommendations Based on Technical Analysis		
Risk Item	**Remediation Recommendation**	**Severity**
Potentially Sensitive Information Contained in SMB Fileshares with Everyone Read/Write Permissions	Review SMB file share permission reports and reduce read/write access for everyone where merited.	Moderate *(Requires [CLIENT] IT Department Verification)*
Lack of WAF on Web App	Consider Implementing Web Application Firewalls	Low
Lack of Observed ACLs Related to VDI Pool	Add Additional ACL Rules to the Standard User VDI pool	Low
SMS MFA Employed - SIM Swapping Attack	Deprecate Support for SMS as an MFA Authentication	Low

In Tabletop scenarios 2 and 3, the lack of implemented web application firewalls increased the probability of success of an APT.

Technical analysis also indicated that the currently enforced ACL rules on standard VDI users allow them to attempt logins on what seem to be potentially significant backup infrastructure devices. Ports associated with protocols FTP, SSH, and TELNET, for example, are open on devices such as REDACTED within the REDACTED Management Appliances subnet. Likewise, legacy data could potentially be accessed through SSH with the computer name “REDACTED” (REDACTED). Unless necessary for the functioning of the day-to-day activities, employees should not be able to attempt to log in to storage infrastructure. By adding additional ACL rules to restrict this for most users, the level of risk of a single compromised system could be reduced.

During tabletop discussions of the scenarios within this engagement, it was identified that although [CLIENT] does enforce multifactor authentication (MFA) on all external systems, SMS is the supported multifactor authentication method. This method can be susceptible to SIM swapping attacks. SIM Swapping attacks are very common and involve an attacker impersonating their target in order to convince their cell phone provider to port the target's phone number to another SIM card. If successful, the target's phone number becomes associated with the SIM card controlled by the attacker. Under this circumstance, if the credentials of that user are compromised, the attacker will be able to bypass an SMS-based MFA control as the MFA code would be sent directly to the attacker's mobile device.



Considering this potential attack vector, Abacus Group recommends slowing phasing out the use of SMS as a supported MFA method. Utilizing time-based one-time passwords (TOTP) via an authenticator application or push notifications on mobile devices are considered to offer a higher degree of security. Additionally, [CLIENT] could consider utilizing a FIDO2 hardware key for either backups or VIP individuals.

Based on these observations, it would be considerably difficult for a malicious actor to gain a foothold into [CLIENT] systems and laterally move fast enough to execute a full-scale cryptolocker ransomware attack (which would require the sabotage of backups and BCDR systems) without setting off security alarms. That said, most high-profile ransomware attacks executed by ATPs like REvil, Conti, Darkside, and Ryuk involve double-extortion or triple-extortion attacks. More specifically, double-extortion and triple-extortion attacks go beyond cryptolocking important corporate files and employ exfiltration of confidential company data, threats of confidential data leakage, and threats of further attacks (sometimes involving DoS attacks). [CLIENT]'s IT department and security team should review SMB file share read/write everyone permissions to ensure the principle of least privilege is employed, and the potential scope of data exfiltration is limited.