Simulated Attack Plan

A Playbook to Simulate Human-Operated Ransomware Attack Activities

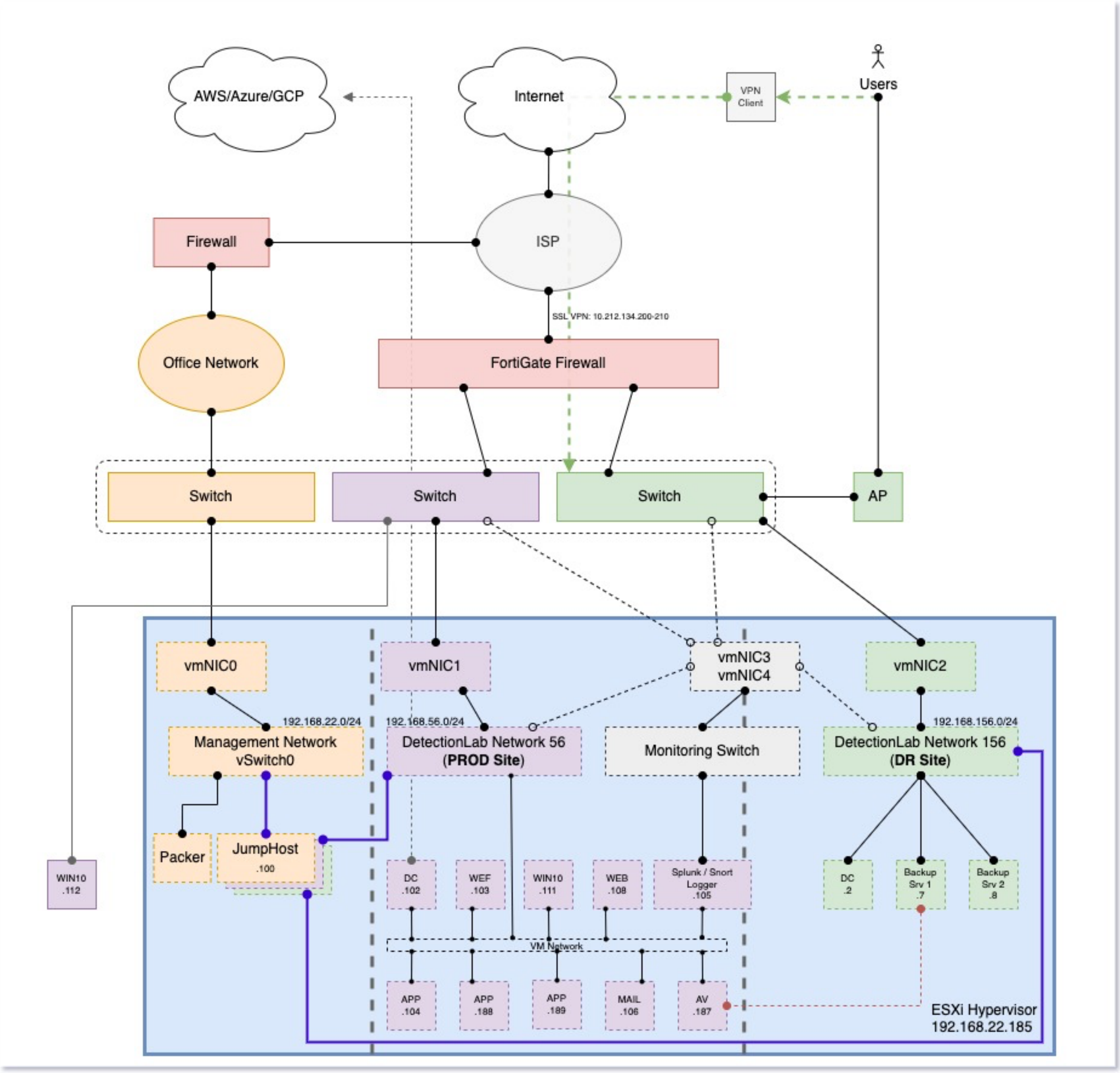
Version 1.0

Release date: 8 Jun 2022

ir@dragonadvancetech.com
Dragon Advance Tech Consulting Company Limited

Table of Contents

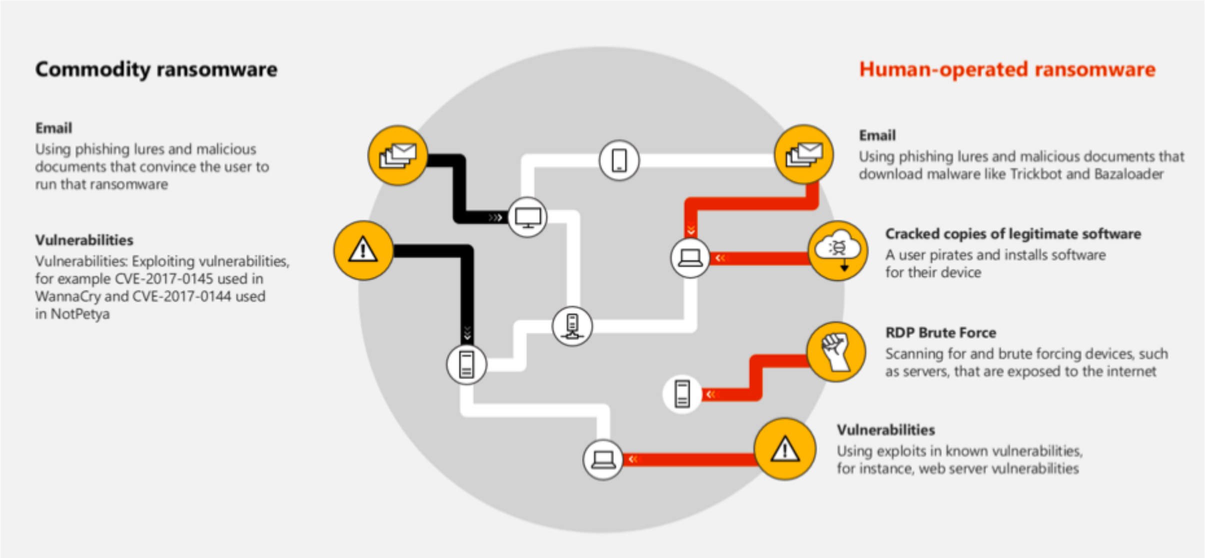
Network Diagram



INTRODUCTION

Extracts from Microsoft Ransomware Hunting Report

Ransomware attacks are a multi-platform threat that continues to impact organizations with little regard for the critical services they might disrupt. These attacks range from highly targeted to opportunistic, depending on the actor's skill set and capabilities. Besides charging ransom, human-operated ransomware actors also look for additional means to leverage pressure on organizations and increase a compromise's profitability. Through data exfiltration and extortion, the attackers increase the likelihood of ransomware payment. While waiting for the price, ransomware actors might drop cryptocurrency miners or create backdoors that give them access to the target (re-pivot back into the infrastructure) even *after the ransom is paid. The following diagram shows an example of known entry points of traditional ransomware and human-operated ransomware activities:*



Commodity ransomware

Email
Using phishing lures and malicious documents that convince the user to run that ransomware

Vulnerabilities
Vulnerabilities: Exploiting vulnerabilities, for example CVE-2017-0145 used in WannaCry and CVE-2017-0144 used in NotPetya

Human-operated ransomware

Email
Using phishing lures and malicious documents that download malware like Trickbot and Bazaloader

Cracked copies of legitimate software
A user pirates and installs software for their device

RDP Brute Force
Scanning for and brute forcing devices, such as servers, that are exposed to the internet

Vulnerabilities
Using exploits in known vulnerabilities, for instance, web server vulnerabilities

BACKGROUND

A security incident happened at ABC company on 27 May.

Fortigate SSL VPN can only access the 192.168.156.0/24 network in the DR site.

There is a log-saving practice on the PR site.

Osquery logs are sent to the logger by fleet via TLS. Windows event logs and Sysmon logs are sent to WEF by Event Subscription, and Windows event logs in certain channels are sent to Splunk in Logger via Universal Forwarder.

Fortigate firewall logs are sent to the Splunk in Logger.

Fortigate firewall firmware version is FortiOS v6.0.

Jump Hosts in DR and PR sites have no signs of being compromised.

HIGH-LEVEL ATTACK PATH

Phase 1 - Initial Access

Exploit the Fortigate firewall vulnerability to gain credentials.

Used the Fortigate SSL VPN as an access point to the network.

I successfully logged in to some machine with the same credential on the DR site.

RDP into a machine and discovered it has access to the PR site.

I was successfully logged in to some machine site with the same credential in the PR site by the pivot machine found above.

Phase 2 – Pre-attack

I was logged in a DC in the PR site by the previous pivot machine found and a DC in the DR site.

Discovered the domain admin credentials in the corresponding machines and RDP in the 2 DCs as the domain admin.

RDP into the previous pivot machine found, and network logon into different machines in the DR site with credentials found.

Phase 3 – Ransomware Attack

Ransomware was deployed to different DR and PR sites using the pivot machine.

LOW-LEVEL ATTACK PATH

Phase 1 - Initial Access

On 10 April at 23:46
VPN login
Exploit the Fortigate with CVE-2018-13374 to gain credentials (*ABCADM01)*.
Use the Fortigate SSL VPN credentials to log in.
Brute force and ping sweep by *Nmap* to find out what network and host VPN has access to.
I discovered the VPN only has a connection to 192.168.156.0/24.
Discovered different hosts are alive.

192.168.156.0/24 Network Reconnaissance
Ran a network scan by port scanning with *Nmap*.
Ran an automatic, organized network reconnaissance by *autorecon.*
Discovered *DC, Backup Server01, Backup Server02*, *VICSS Server,* and *Jump Host* inside 192.168.156.0/24.

***Backup Server01* has access to** 192.168.56.0/24
Discovered a machine *Backup Server01* belongs to a domain *abcdomain.com* while others are not.
Password spraying to a different protocol (LDAP, Winrm, RDP) with the VPN credentials (*ABCADM01*) inside the network (192.168.156.0/24) by *CrackMapExec*.
Backup Server01 has an IP of 192.168.156.7.
I discovered that the account *ABCUSR01* can RDP into *Backup Server01.*
ABCUSR01 is a domain user.
I discovered that *Backup Server01's* DNS server, dc.abcdomain.com has an IP of 192.168.56.102, implying that *Backup Server01* could reach 192.168.156.0/24 and 192.168.56.0/24.

192.168.56.0/24 Network Reconnaissance by *Backup Server01*
Brute force and ping sweep by *CMD commands* to determine what machines in 192.168.56.0/24 *Backup Server01* could reach.
Gather information about the domain by *nltest.*
Discovered *DC*, *SCS Server, Mcafee ePo AV Server, SCS Server, VICS Server, WEF, Logger,* and *Jump Host* inside 192.168.56.0/24.
Password spraying to a different protocol (LDAP, Winrm, RDP) with the same credentials inside the 192.168.56.0/24 by running *DomainPasswordSpray.ps1* from PowerShell without downloading.
I successfully logged in to *Mcafee ePo AV Server* and a *SCS Server*.

Phase 2 – Pre-attack

On 15 May at 23:37
I am getting the credentials of the Fortigate SSL VPN on the Dark Web.
Login the SSL VPN and RDP into the ***Backup Server01*** as ABCUSR01.
Weaponizing in *Backup Server01*
I successfully logged in to the Control panel of Mcafee ePo AV with the same credentials.
And turned off the Mcafee ePo AV on ***Backup Server01***.

Transferring Tools including *Defender Control, Mimikatz, winpeas, windows-exploit-suggester.py, and pupy generated payload shell by RDP.*

Leveraging *Backup Server01*
Port scan the machines inside 192.168.56.0/24 with Nmap by tunneling.
Disabling the Windows Defender in *Backup Server01* by Defender Control.
Run the *BloodHound* on the attack machine to gather Domain information.
Run *winpeas* and *windows-exploit-suggester.py* for possible privilege escalation methods but failed to find one.
Run the *pupy* payload and connect the shell back to the attack machine.
Run the bypassuac module embedded in the *pupy* payload shell.

Lateral movement and Looting
Successfully escalated the privilege by bypassinguac.
Add a domain admin account and grant all the rights to *ABCADM04* for later actual attack or backup*.*
Run *powerView* and *mimikatz* modules embedded in the pupy escalated shells.
PowerView gained some information about the domain, and *mimikatz* managed to capture account and password hashes.

JohnTheRipper inside the attack machine can crack some password hashes, including *ABCADM02 and ABCADM03.*

Password spraying to different protocols (LDAP, Winrm, RDP) with the *ABCADM02* and *ABCADM03* credentials inside the 192.168.56.0/24 and 192.168.156.0/24 by running *DomainPasswordSpray.ps1* from PowerShell without downloading.
ABCADM02 can ssh into *WEF*, *Logger* inside 192.168.56.0/24.
ABCADM03 can RDP into the *VICS Server* and *SCS servers* inside 192.168.56.0/24 and *Backup Server02* and *VICSS server* inside 192.168.156.0/24.

Use *PowerShell* to search for standard document extension files, zip it into a file, and transfer the file back to the attack machine by RDP.

Perform reconnaissance, disabling Mcafee ePo AV, weaponization, looting, and cleaning up the tools and the collected files by *SDelete.exe* in every machine that we have access.
Later, a similar attack path can be repeated by bypassing UAC by elevating the ABCADM03 shell in Backup Server02 and VICSS server in 192.168.156.0/24.

Enabling back Mcafee ePo AV on all machines before logging out.

Phase 3: The Ransomware Attack

On 27 May at 23:16
Login the SSL VPN and RDP into the ***Backup Server01*** as ABCAMD01.

Ransomeware attack

Use PsExec to transfer the ransomware binary to all machines in 192.168.56.0/24 except the *jump host* and execute the ransomware as *ABCADM04*.
Use PsExec to transfer the ransomware binary to all machines in 192.168.156.0/24 except the *jump host* and execute the ransomware as *ABCADM03.*