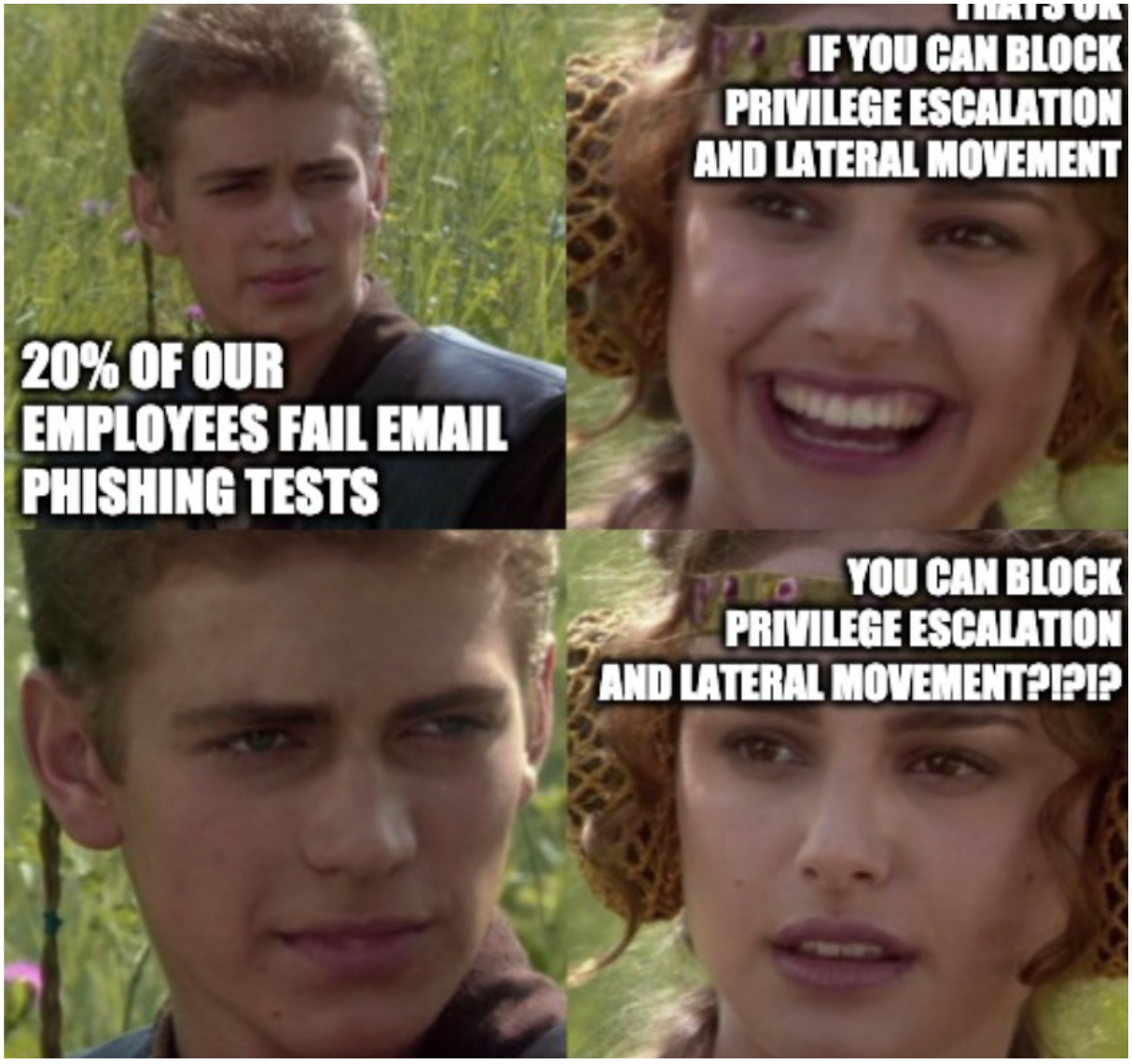
What We Can Learn From Ransomware Actor "Security Reports"



“How did they get in? When will we know?”

These are among the most common questions we hear in the initial aftermath of a ransomware attack and with good reason. Not only does the victim organization want to understand what led to the devastating attack, they want to explain to their employees and stakeholders how they've contained the incident and reassure them that the problem won't recur. Focusing on just the point of ingress has also been magnified by the recent high profile attacks that have captivated the attention of regulators, lawmakers and heads of state. It's usually too simple to proclaim that "a single weak password..." caused a systemic incident. Fortunately, threat actors commonly describe and brag about their attack techniques and some will even provide structured reports.

Since 2018, big game hunting ransomware actors have set their sights to bigger and more lucrative enterprise targets. In order to pull off an attack of this magnitude, they need to come prepared. It's not just about getting in. It's about staying in, enumerating the network and backing up resources so the attack is nearly impossible to thwart, and hard to recover from without experiencing serious business interruption. On the defender's side, the internet is stocked with resources that describe how to build 'defense in depth.' Additionally, defenders can learn directly from the threat actors themselves; descriptions of their own attack techniques provide a unique window into what happens between initial ingress and detonation.

The complexity and expense of big game attacks have led to heightened ransom demands. It is not uncommon for threat actors to try to entice victims into a payment by adding a "security report" to sweeten the deal. They know victims are keen to understand how the attack happened and how to prevent it moving forward. Of course, we prefer to rely on trusted forensic investigation for these reports, but in practice many variables complicate the confidence of forensic conclusions: machines are wiped in a rush to restore operations, evidence is overwritten, and/or threat actors run wiping utilities to hide footprints. In short, even though trusted forensic investigators are more qualified to offer cybersecurity best practices, threat actor reports are valuable resources for understanding how ransomware attacks occur and what can be done to prevent them.

Before we dig into reports that have provided useful information, it is important to note that not all "security reports" offer actionable information. The quality and utility of the reports is inconsistent between ransomware groups. For example, Conti and SunCrypt ransomware consistently produce the same vague, 3-4 boilerplate

sentences to all victims without commenting on the details of initial attack methods. Other variants like Mespinoza can often only be bothered to supply a few words.

Luckily, some threat actors are more forthcoming. What follows are several case studies from real ransomware negotiations wherein the threat actor provided granular details on the full attack lifecycle, including usernames and passwords of compromised accounts and specific CVE's leveraged to gain entry. Please note that these reports have not been edited or spell checked and that we redacted identifying information. Additionally, the tactics described by the threat actors herein were validated following thorough forensic investigation.

Babuk Ransomware Case Study

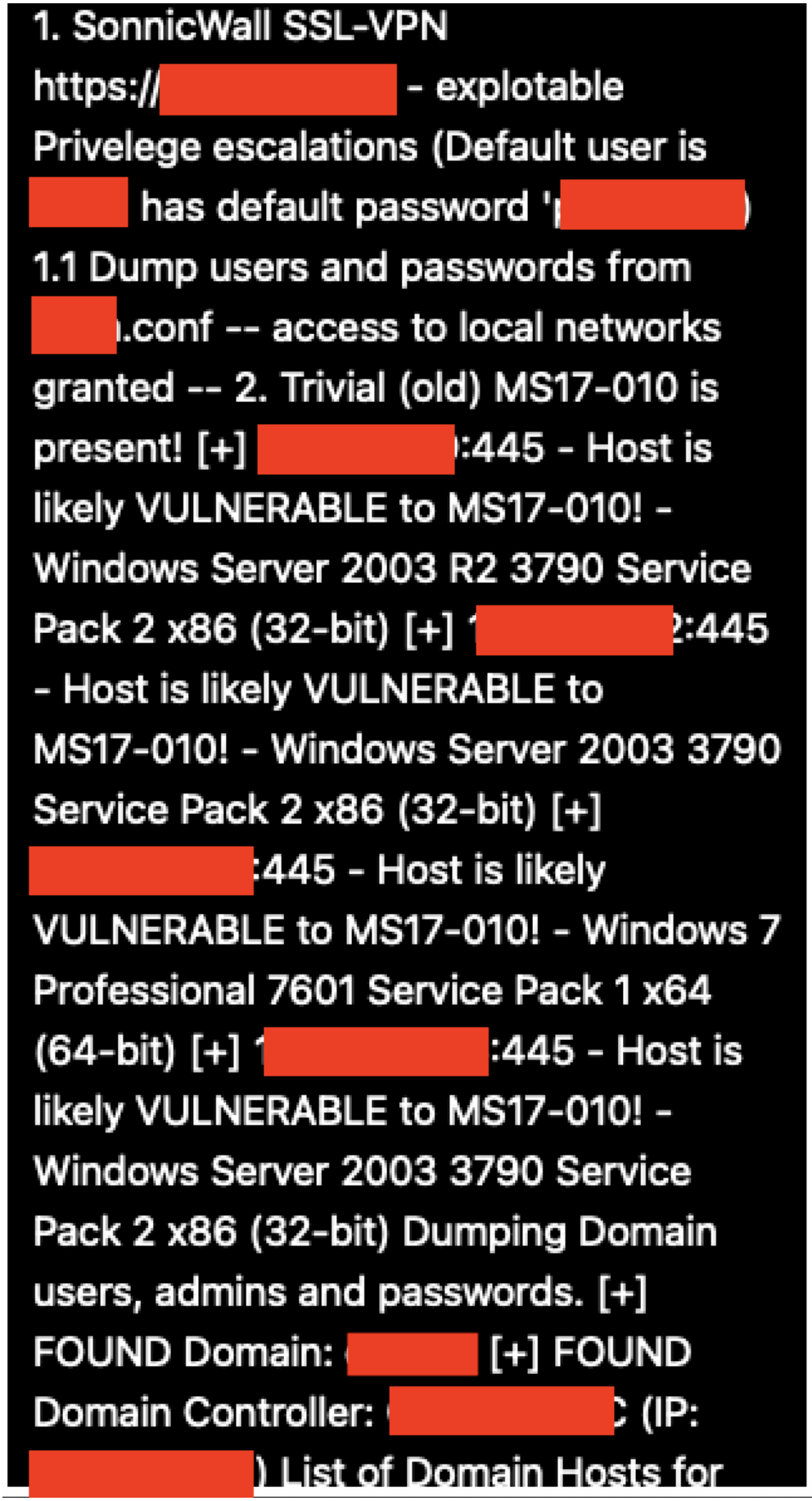

1. SonnicWall SSL-VPN
https://
- explotable
Privelege escalations (Default user is
has default password '
1.1 Dump users and passwords from
.conf -- access to local networks
granted -- 2. Trivial (old) MS17-010 is
present! [+]
:445 - Host is
likely VULNERABLE to MS17-010! -
Windows Server 2003 R2 3790 Service
Pack 2 x86 (32-bit) [+]
:445
- Host is likely VULNERABLE to
MS17-010! - Windows Server 2003 3790
Service Pack 2 x86 (32-bit) [+]
:445 - Host is likely
VULNERABLE to MS17-010! - Windows 7
Professional 7601 Service Pack 1 x64
(64-bit) [+]
:445 - Host is
likely VULNERABLE to MS17-010! -
Windows Server 2003 3790 Service
Pack 2 x86 (32-bit) Dumping Domain
users, admins and passwords. [+]
FOUND Domain:
[+] FOUND
Domain Controller:
(IP:
) List of Domain Hosts for

Figure 2. Excerpt from Babuk report. Full redacted text transcribed below.

1. SonnicWall SSL-VPN

https://[redacted] - explotable Privelege escalations (Default user is '[redacted]' has default password '[redacted]') 1.1 Dump users and passwords from [redacted].conf -- access to local networks granted -- 2. Trivial (old) MS17-010 is present! [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 2 x86 (32-bit) [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit) [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit) [+] [redacted]:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit) Dumping Domain users, admins and passwords. [+] FOUND Domain: [redacted] [+] FOUND Domain Controller: [redacted]-DC (IP: [redacted]) List of Domain Hosts for the primary Domain. ========== Domain Hostname IPs ------ -------- ---

[redacted list of hostnames and IPs]

Antivirus software don't block payloads 3.1 Antivirus software can be deactivate 4. Data shared without strong restrictions! 4.1 Critical data wasn't encrypted.

INGRESS

In this Babuk case, the threat actor leveraged an unpatched vulnerability in the victim's SonicWall VPN. Although they omit the precise CVE, CVE-2020-5135 is a likely candidate - it was announced in October 2020 and continues to be heavily abused by ransomware groups today.

ESCALATION

Once they're in, the next step is almost always related to credential harvesting. Having a complicated unguessable password isn't much help if the bad actor is already inside and stealing it in plaintext. While they are usually focused on hijacking the domain administrator accounts for attack staging purposes, having access to the entire library of users is important for redundancy in case their primary access gets thwarted. The threat actor also points out the network is home to *numerous* legacy systems that are vulnerable to MS17-010 aka the EternalBlue SMB

exploit. This exploit was implicated in the infamous WannaCry ransomware attacks of 2017, which allowed bad actors to push malware throughout enterprise networks with little effort.

LATERAL MOVEMENT

After moving between endpoints using internal Remote Desktop Protocol (RDP), the threat actor found what they were looking for, the domain controller. From there, they enumerated the full list of hosts on the available network. Whether setting up a group policy, scheduling a task, or using PsExec to copy/paste payloads, having a comprehensive host list is a necessity to attack at the enterprise level.

IMPACT

The threat actor leveraged a quiet software vulnerability to gain initial entry - a step that's unlikely to set off alarm bells on its own. By taking ownership of a root user with a default password, they were able to conduct the credential harvesting and basic network mapping to detonate their ransomware. The threat actor proudly announces their malware payload goes undetected by standard signature-based antivirus, but nonetheless points out that any user on the victim's AV console can deactivate the software. You might have the best endpoint protection in the world, but if it doesn't require authentication to disable it, its utility is limited. Before setting off the ransomware, they scraped 500gb of sensitive data from the file server to hold as additional leverage. Fortunately, in this case, they *did not* succeed in encrypting the victim's incremental backups.

MITRE TACTICS

The attack in this case can be mapped to the following MITRE ATT&CK® Tactics.

T1190: Exploit Public-Facing Application

T1003: OS Credential Dumping

T1078.002: Valid Accounts: Domain Accounts

T1059: Command and Scripting Interpreter

T1021:002: SMB/Windows Admin Shares

T1210: Exploitation of Remote Services

T1087: Account Discovery

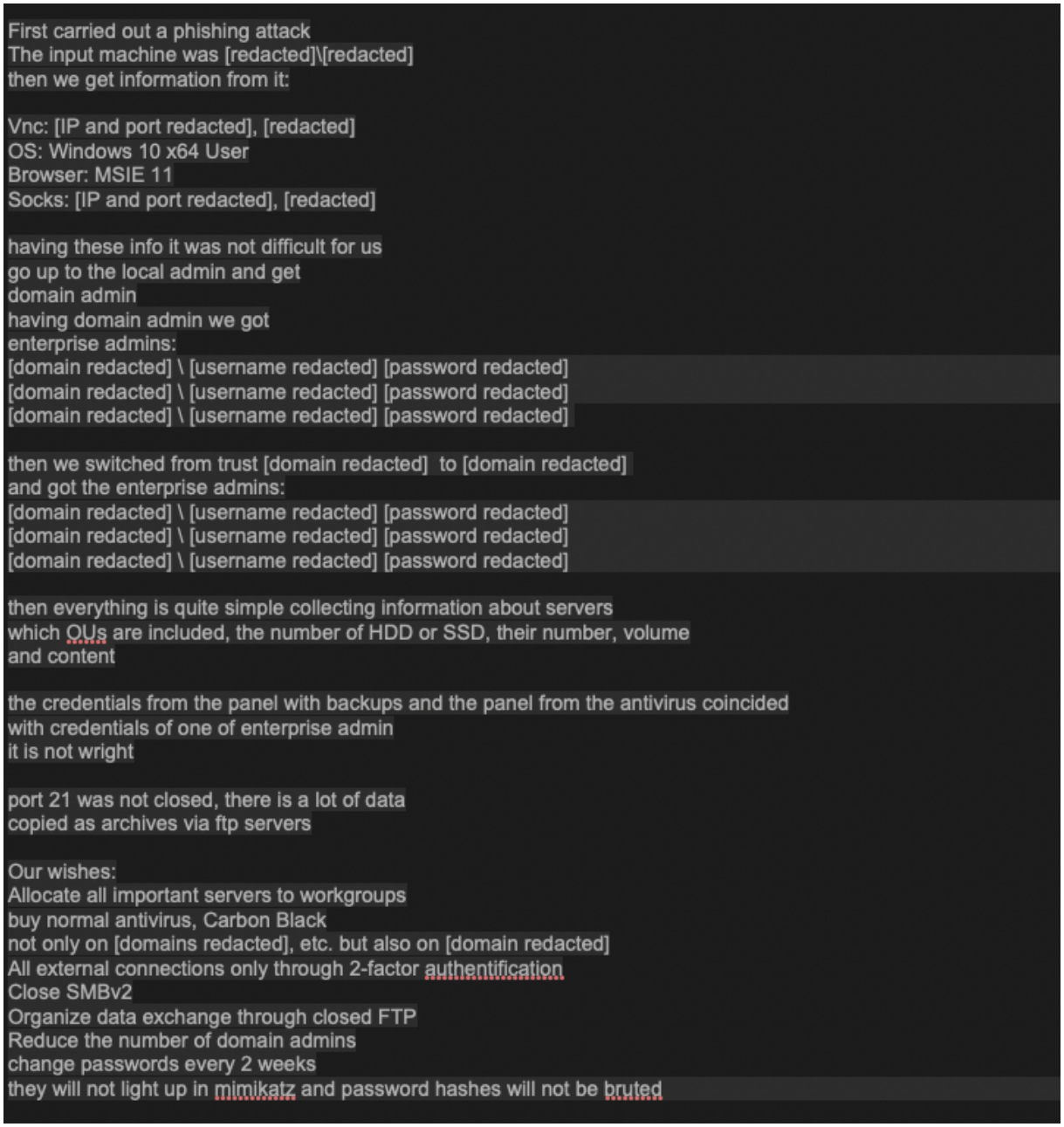
T1482: Domain Trust Discovery

T1562: Impair Defense

T1537: Transfer Data to Cloud Account

T1567: Exfiltration Over Web Service

Lone Wolf (unaffiliated) Group Case Study



INGRESS

Like many other case studies, initial ingress was achieved via a single end user workstation. A phishing attack was successfully executed on this host (domain and hostname redacted for this report, but included in actual transcript). Although the threat actor did not explicitly state whether the delivery mechanism was a weaponized attachment or a malicious link, basic forensic artifacts would allow the investigator to narrow down the method.

ESCALATION

Using just the details gleaned from the initial workstation, the threat actor identified VNC and SOCKS authentication details (IP, port, password), and moved from the original compromised user to **six** domain administrator users (usernames/passwords redacted).

PERSISTENCE

The threat actor identified that the same credentials used to manage the backups were also being used to control the antivirus software. In one motion they are able to gain control of the backups for the purpose of encrypting them, and simultaneously disable antivirus protection to squash any potential detections from giving away their attack staging.

IMPACT

This is one of the only threat actor reports received to date that addressed data exfiltration methods. TCP Port 21 (associated with file transfer protocol) was left open at the time of the attack and allowed the threat actor to move files out of the network with ease. In this case, the threat actor exfiltrated an extremely large volume of highly sensitive data from the victim. They fully encrypted the majority of the company's production servers. They also encrypted most of the company's backups, and wiped a substantial portion of other backup systems.

MITRE TACTICS

T1566: Phishing

T1219: Remote Access Software

T1003: OS Credential Dumping

T1210: Exploitation of Remote Services

T1087: Account Discovery

T1078.002: Valid Accounts: Domain Accounts

T1562: Impair Defense

T1048: Exfiltration Over Alternative Protocol

T1486: Data Encrypted for Impact

Egregor Ransomware Case Study

"Security report - Initial access was gotten from phishing email, then we make harvesting information about active directory groups and rights using LDAP protocol using bloodhound. Then, having user token of call center we got access to other computers from this group of user using protocol WinRM. On every computer we have executed mimikatz, which dumped NTML hash of user [Redacted UserName]. This user was in group of Domain Admins. For persistence we created user "[Redacted DA Name]" and added it into all groups containing domain admins. After we got the full access of the network, we began looking the info about the company. Server [Redacted Server name] was the mirror of cluster [Redacted Cluster Name]. In the folder users were the table with passwords for a root account of [Redacted Server name] panel. File was [REDACTED]. It had passwords to four [Redacted Cluster Name]: [Redacted Cluster Name1 [Redacted Cluster Name2][Redacted Cluster Name3][Redacted Cluster Name4], From [Redacted] clusters we downloaded all information and deleted all snapshots."

INGRESS

The threat actor used a phishing email to install a Remote Access Trojan (RAT) on a single employee's computer. Note the RAT is not mentioned in the security report, but that was how they were able to login to this single machine.

ESCALATION

The threat actor mentions in third sentence that *"on every computer we have executed mimikatz, which dumped NTML hash of user [redacted]…his user was in group of Domain Admins."* This is where the serious trouble begins, as now the threat actor has domain admin credentials. With these senior credentials, and no multifactor authentication to stop them, they are free to move around the network.

LATERAL MOVEMENT

The threat actor leverages a network enumeration tool called Bloodhound to discover company assets that they can move between using escalated privileges. In this case, the early compromise of domain admin credentials made lateral movement extremely easy for this threat actor.

PERSISTENCE

Rather than using the compromised domain admin credentials while in the network, the threat actor opted to create a new set of equally senior domain admin credentials, and added this domain admin user to all the domain admin groups in the victims active directory. This ensured that the actual domain admin user of the compromised credentials would not notice or unexpectedly kick the threat actor out by logging in simultaneously.

IMPACT

The threat actor used their vast lateral range and domain admin credentials to wipe the company's backups, steal several hundred gigabytes of data. As a final act, they disabled antivirus and endpoint detection, and used a group policy to detonate the encryption ransomware on every endpoint they could access (which was pretty much every server and desktop in the network).

MITRE TACTICS

T1566: Phishing

T1219: Remote Access Software

T1003: OS Credential Dumping

T1059: Command and Scripting Interpreter

T1021.006: Windows Remote Management

T1087: Account Discovery

T1136: Create Account

T1078.002: Valid Accounts: Domain Accounts

T1562: Impair Defense

T1567: Exfiltration Over Web Service

T1485: Data Destruction

T1486: Data Encrypted for Impact

ClоP (now in cuffs) Ransomware Case Study

“This report will allow you to protect your network from the slack of a large part of the evil people, but it does not give 100% guarantee that no one will ever hack you again. We got into your network through Phishing. The email with the malicious attachment was opened by an employee working on a PC with a name [Redacted]. If you open an email, the user is asked to include the document's macro, to display the content, click on the link, etc. - know this bad writing. It’s very difficult and practically impossible to teach or force company users not to open such emails, it’s also difficult to monitor this. #Solution: network Administrators should make it impossible to perform such an attack! And users will be calm #How? You should figure it out for yourself. You can open email clients and browsers in virtual machines, for example, by restricting the launch of executable code, system commands, and services.

After gaining access to the PC and a successful fixer in system, we've started collecting technical information about your network. 1. List of PCs and their IP addresses in your network. #attention to the prohibition of LDAP requests 2. Preenity of domain administrators. It was the first phase of the attack on yours. Any malicious person who has got into the network of the organization the first task of raising privileges. We used uac-token-duplication exploit to get system privileges

Dump password hashes local Administrator

[Redacted Hash]

These hashes have allowed us to carry out pass-the-hash attacks and will spread horizontally on your network with maximum pc rights where the passwords of local administrators coincide with the password installed on the PC Local Administrator success access to [Redacted IP address] pc [Redacted IP] address have credentials corp\[Redacted] corp\[Redacted] success access to [Redacted IP address] and [Redacted IP address] have credentials Domain Admins. With the administrator password, we have full access to your domain and trust domains, respectively. Already at this stage, your administrators may have made it difficult for us to work, but they

made trivial mistakes in their work. For your safety I want to give my recommendations."

INGRESS

The CloP threat actors used a phishing email that contained an attachment with a malicious macro (who needs 0-days, when excel files with macros still work!). The macro that was enabled by the user was a malicious process that pulled malware onto the users machine, and enabled the threat actor to gain remote access.

ESCALATION

The threat actor leveraged LDAP requests to find user lists from the local machine. These requests don't give them full credentials, but they first get a list of administrative credentials via these lists. Once the threat actor knows what admin user names they want to target they use Metasploit's Meterpreter payload to do token impersonation to escalate privileges on the administrative accounts that were compromised.

LATERAL MOVEMENT

The threat actor notes that since local administrators had the same rights as network admins, they were able to move laterally between several hosts, and repeat their hash dumping and token impersonation. They repeated this process until they uncovered a set of domain admin credentials.

PERSISTENCE

The threat actor did not need to maintain a great deal of persistence on this case as data exfiltration was their primary motive. Once they had removed enough data from the victims network, they did not return.

IMPACT

The threat actor used their domain admin credentials to steal about 500 gigabytes of sensitive data from this victim.

MITRE TACTICS

T1566: Phishing

T1204.002: User Execution: Malicious File

T1548: Abuse Elevation Control Mechanism

T1550.002: Use Alternate Authentication Material: Pass the Hash

T1059: Command and Scripting Interpreter

T1087: Account Discovery

T1563: Remote Service Session Hijacking

T1482: Domain Trust Discovery

T1078.002: Valid Accounts: Domain Accounts

T1537: Transfer Data to Cloud Account

T1486: Data Encrypted for Impact

Make your Organization an Expensive Target

For those responsible for securing networks, it is CRITICAL to look beyond the point of ingress. Having tunnel vision on preventing phishing emails, misses the most important phase of the attack life cycle - the days, weeks, and sometimes months, of activity that take place *between* the initial entry and the ultimate attack detonation. This middle stage is a critical line of defense where many ransomware battles are either won or lost by enterprises.

In reviewing these case studies the repetition of tactics is obvious. Why do threat actors repeat themselves? Because they are profit driven, and what they are currently doing works. It would be economically irrational to try new and time consuming tactics when their practiced techniques are effective. With the exception of purchasing initial access credentials on the dark web, all the other tactics described in these cases leverage free offensive tools such as Mimikatz, Cobalt Strike, or Metasploit. No expensive zero days, or custom malware was used in these attacks.

Again, please note that blocking EVERY phishing email, or patching every access vulnerability is NOT feasible and it is likely that some of these actors are going to get in. Therefore, the logical next step is

making it TOO expensive for them to escalate and move around laterally. Organizations that have expansive depth in the middle, are less likely to suffer catastrophic business interruption. Given the consistent and well-observed attack techniques, there are correspondingly effective defense techniques that will make your organization too expensive for ransomware actors.

Top 3 ways to stop a potential ransomware attack (along with the MITRE Mitigation ID)

1. **Use multi factor authentication on your domain administrator accounts.** We mean REAL multi factor authentication via authentication codes accessed by use of a username, complex rotating PW, and authentication codes only accessible with the users mobile device. Coveware has NEVER seen a ransomware attack, where domain administrator credentials were compromised after multifactor authentication (mobile, not token based) was overcome. 100% of ransomware attack victims LACK true multi factor authentication for the domain administration accounts. M1032
2. **Disable command-line and scripting activities from every machine possible.** As you will note from the above reports, threat actors are heavily reliant on free software utilities that run from the command line. If they are NOT able to run these tools, they will have a difficult time escalating privileges and/or moving laterally. M1026, M1042 and M1038
3. **Segment your network**. A flat, unsegmented network is like keeping all your most valuable assets in the same location. Network segmentation makes valuable assets harder to find, and thus compromise. M1030