Ransomware Delivered Using RDP Brute-Force Attack

zscaler.com/blogs/security-research/ransomware-delivered-using-rdp-brute-force-attack

Zscaler ThreatLabZ recently published a report on the 2020 State of Public Cloud Security that showed security misconfiguration to be the leading cause of cyberattacks against public cloud infrastructure. In this blog, we will look at one of the commonly abused security misconfigurations—the RDP service port left open to the internet—and how cybercriminals abuse it.

Brute-forcing RDP (Remote Desktop Protocol) is the most common method used by threat actors attempting to gain access to Windows systems and execute malware. The reason is simple: In our public cloud threat research, we have observed that 70 percent of systems keep RDP ports open in the public cloud. Threat actors scan for these publicly open RDP ports to conduct distributed brute-force attacks. Systems that use weak credentials are easy targets, and, once compromised, attackers sell access to the hacked systems on the dark web to other cybercriminals.

Ransomware groups such as SamSam and Dharma have been spreading almost exclusively via RDP for years. In this case study, we will look at Dharma ransomware attacks. Dharma, also known as Crysis, has been distributed under a ransomware-as-a-service (RaaS) model since 2016. Its source code was up for sale in March 2020, making it available to a wider spectrum.

Infection chain

Attackers use open-source port-scanning tools to scan for exposed RDP ports online and then try to gain access to a system using brute-force tools or stolen credentials purchased from the dark web. After attackers gain access to the target system, they go on to make the system vulnerable by deleting backups, disabling antivirus software, and changing configuration settings. Once the security is disabled and the network vulnerable, attackers deliver malware payloads. The process involves installing ransomware, using infected machines to distribute spam, deploying keyloggers, or installing backdoors to be used for future attacks.

The below figure shows the infection cycle of Dharma ransomware delivered via RDP brute-force attack.

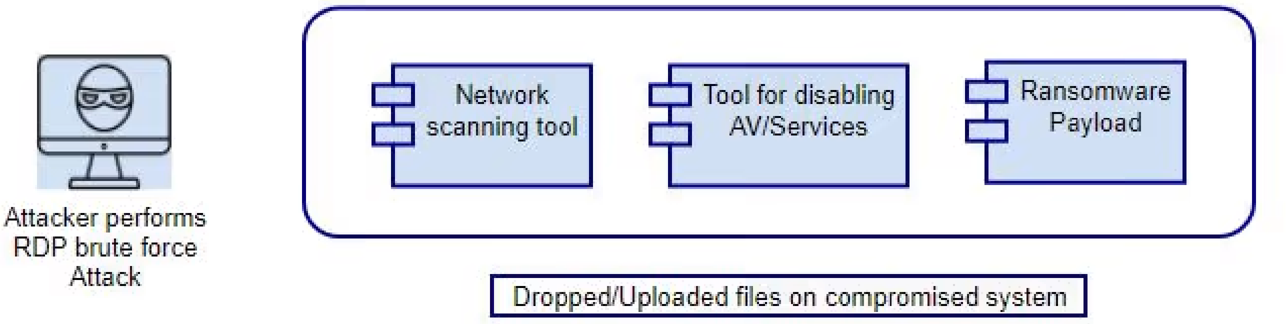

Attacker performs RDP brute force Attack
Network scanning tool
Tool for disabling AV/Services
Ransomware Payload
Dropped/Uploaded files on compromised system

Figure 1: Infection chain of RDP brute-force attack delivers Dharma ransomware

Once the attacker gains access to the machine, the following files are uploaded:

%temp%\ns.exe – Network enumeration/scanning tool

%programfiles%\process hacker\ – Process hacker tool

ns.exe is a network enumeration and scanning tool used by attackers to scan SMB shares, open ports, and services through which they can move within the network.

Process Hacker is a program used mostly by system administrators for monitoring, debugging, and troubleshooting, but in this case, it was used for malicious purposes such as disabling AV or services.

Following the pre-execution process, the attacker uploads a ransomware file and executes it.

Technical details

Once executed, this variant of Dharma ransomware uses the below commands to quietly delete all of the shadow volume copies on the machine.

mode con cp select=1251

vssadmin delete shadows /all /quiet

Exit

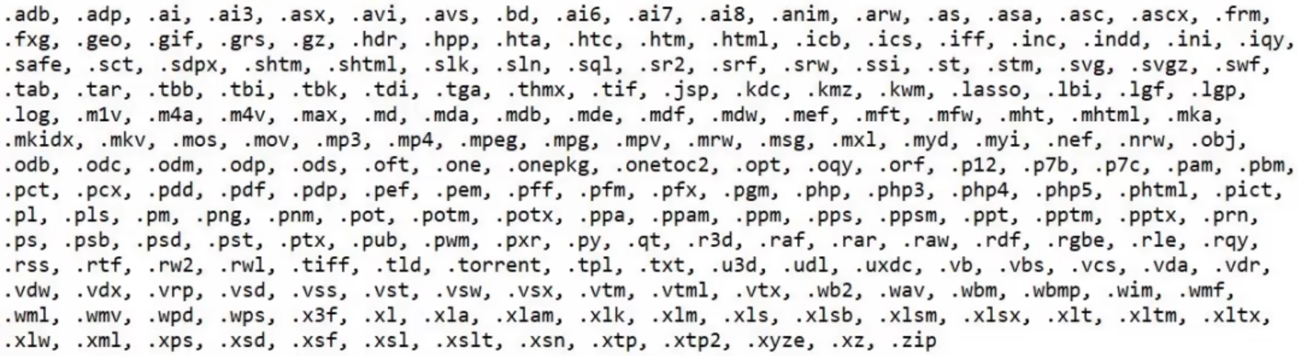
For persistence, the ransomware executes the following commands:

1. Copy the file to *%windir%system32* or *%appdata%* and set *'LOCAL_MACHINE/LOCAL_USER Software\Microsoft\Windows\CurrentVersion\Run'*

2. Copy file to 'Startup' folder

3. Copy file to 'Common Startup' folder

The ransomware encrypts files with the following extensions:



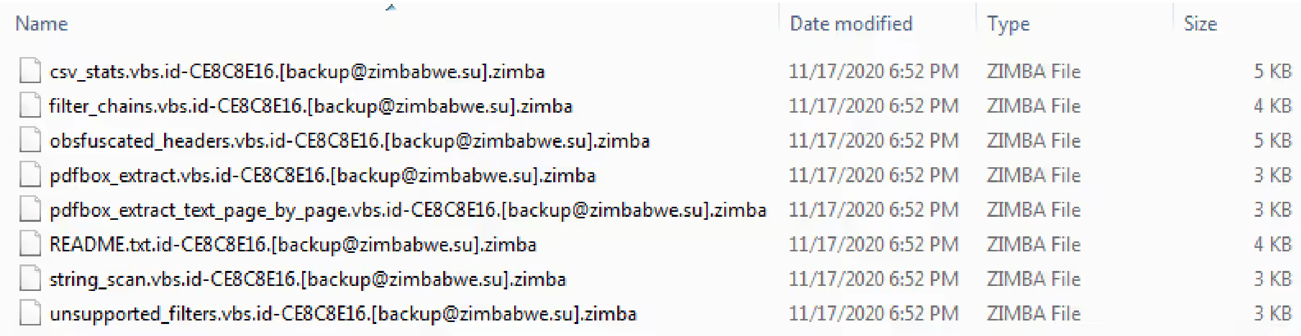
```
.adb, .adp, .ai, .ai3, .asx, .avi, .avs, .bd, .ai6, .ai7, .ai8, .anim, .arw, .as, .asa, .asc, .ascx, .frm,
.fxg, .geo, .gif, .grs, .gz, .hdr, .hpp, .hta, .htc, .htm, .html, .icb, .ics, .iff, .inc, .indd, .ini, .iqy,
.safe, .sct, .sdpx, .shtm, .shtml, .slk, .sln, .sql, .sr2, .srf, .srw, .ssi, .st, .stm, .svg, .svgz, .swf,
.tab, .tar, .tbb, .tbi, .tbk, .tdi, .tga, .thmx, .tif, .jsp, .kdc, .kmz, .kwm, .lasso, .lbi, .lgf, .lgp,
.log, .m1v, .m4a, .m4v, .max, .md, .mda, .mdb, .mde, .mdf, .mdw, .mef, .mft, .mfw, .mht, .mhtml, .mka,
.mkidx, .mkv, .mos, .mov, .mp3, .mp4, .mpeg, .mpg, .mpv, .mrw, .msg, .mxl, .myd, .myi, .nef, .nrw, .obj,
.odb, .odc, .odm, .odp, .ods, .oft, .one, .onepkg, .onetoc2, .opt, .oqy, .orf, .p12, .p7b, .p7c, .pam, .pbm,
.pct, .pcx, .pdd, .pdf, .pdp, .pef, .pem, .pff, .pfm, .pfx, .pgm, .php, .php3, .php4, .php5, .phtml, .pict,
.pl, .pls, .pm, .png, .pnm, .pot, .potm, .potx, .ppa, .ppam, .ppm, .pps, .ppsm, .ppt, .pptm, .pptx, .prn,
.ps, .psb, .psd, .pst, .ptx, .pub, .pwm, .pxr, .py, .qt, .r3d, .raf, .rar, .raw, .rdf, .rgbe, .rle, .rqy,
.rss, .rtf, .rw2, .rwl, .tiff, .tld, .torrent, .tpl, .txt, .u3d, .udl, .uxdc, .vb, .vbs, .vcs, .vda, .vdr,
.vdw, .vdx, .vrp, .vsd, .vss, .vst, .vsw, .vsx, .vtm, .vtml, .vtx, .wb2, .wav, .wbm, .wbmp, .wim, .wmf,
.wml, .wmv, .wpd, .wps, .x3f, .xl, .xla, .xlam, .xlk, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx,
.xlw, .xml, .xps, .xsd, .xsf, .xsl, .xslt, .xsn, .xtp, .xtp2, .xyze, .xz, .zip
```

Figure 2: File extensions to encrypt

The ransomware encrypts files using an AES 256 algorithm. The AES key is also encrypted with an RSA 1024 algorithm. This encrypted AES key is stored at the end of the encrypted file along with the filename.

The name of the encrypted files have the following pattern:

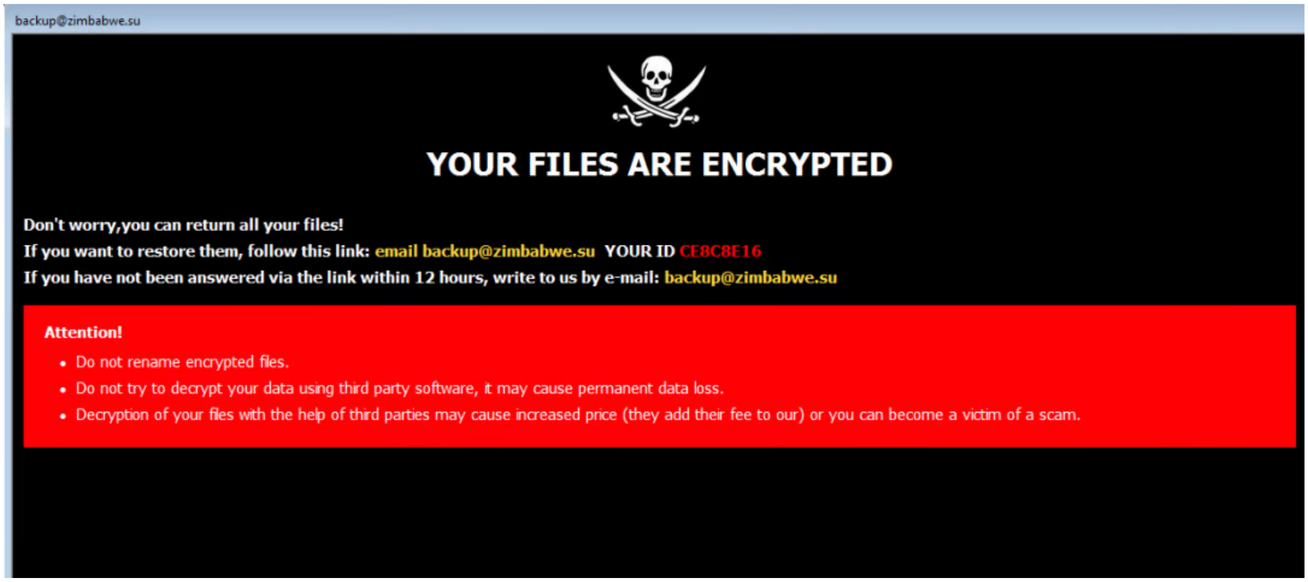
[Filename].id-{8 bytes ID}.[recovery_email].zimba



Name	Date modified	Type	Size
csv_stats.vbs.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	5 KB
filter_chains.vbs.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	4 KB
obsfuscated_headers.vbs.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	5 KB
pdfbox_extract.vbs.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	3 KB
pdfbox_extract_text_page_by_page.vbs.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	3 KB
README.txt.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	4 KB
string_scan.vbs.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	3 KB
unsupported_filters.vbs.id-CE8C8E16.[backup@zimbabwe.su].zimba	11/17/2020 6:52 PM	ZIMBA File	3 KB

Figure 3: Encrypted files

After encrypting the files, the ransomware pops up two different ransom notes on the victim's computer. One is the *Info.hta* file, which is launched via autorun when a user logs into the computer.



YOUR FILES ARE ENCRYPTED

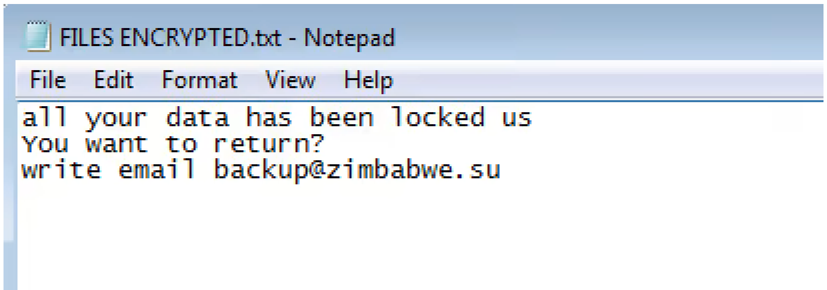
Don't worry,you can return all your files!
If you want to restore them, follow this link: email backup@zimbabwe.su YOUR ID CE8C8E16
If you have not been answered via the link within 12 hours, write to us by e-mail: backup@zimbabwe.su

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: info.hta

The other note is called FILES ENCRYPTED.txt and can be found on the desktop.



```
all your data has been locked us
You want to return?
write email backup@zimbabwe.su
```

Figure 5: FILES ENCRYPTED.txt

Lateral movement

Dharma ransomware uses typical methods for obtaining credentials and propagating laterally within a network. In most cases, it uses the Mimikatz tool, which allows it to dump the network share credentials, and in other cases, it uses NirSoft CredentialsFileView, which allows for the recovery of passwords stored in encrypted credential files. The obtained credentials are used to attempt lateral movement inside the on-prem as well as public cloud infrastructure.

In some cases, the ransomware tries to spread through the network by taking advantage of the compromised Domain Controller and deploying a Default Domain Policy that will run the ransomware payload on StartUp for each machine.

Conclusion

Since Dharma ransomware is usually installed by gaining access to Remote Desktop Services, it is important to ensure that those services are properly locked. This includes ensuring that computers running Remote Desktop Services do not connect directly to the internet. Instead, organizations should use a zero trust architecture to allow remote users to securely access these servers without exposing them to the entire internet.

While applying security patches is always important, most RDP-based attacks rely on cracking weak credentials, so passwords should be long, unique, and random. It's important for enterprises to establish password requirements and train employees to use strong passwords.

Attackers typically identify potential targets by scanning the internet for systems listening on the default RDP port (TCP 3389). Changing the listening port via Windows Registry can help organizations hide vulnerable connections.

MITRE ATT&CK tactic and technique mapping

Tactic	Technique
T1190	Exploit Public-Facing Application
T1059	Command Line Interface
T1061	Graphical User Interface
T1547	Boot or Logon Autostart Execution
T1037	Startup Items
T1110	Brute Force
T1003	Credential Dumping
T1083	File and Directory Discovery
T1135	Network Share Discovery
T1018	Remote System Discovery
T1063	Security Software Discovery
T1076	Remote Desktop Protocol
T1105	Remote File Copy
T1486	Data Encrypted for Impact