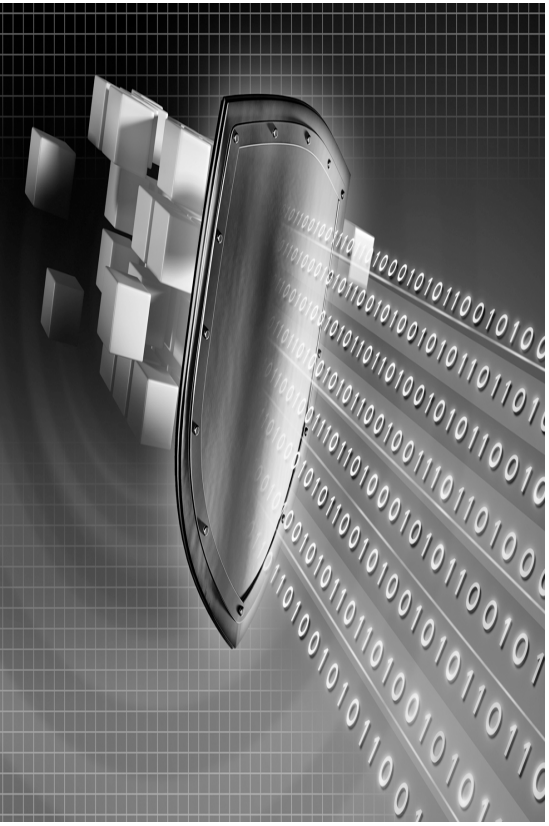
RSA FirstWatch

The VOHO Campaign

An In Depth Analysis



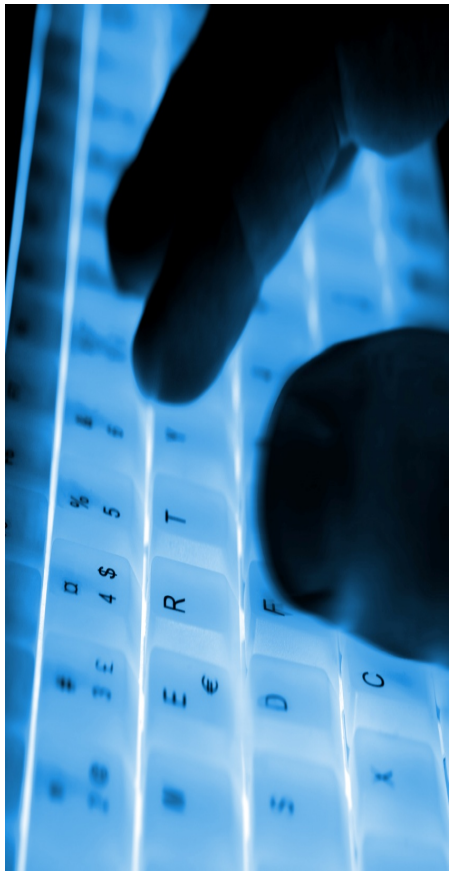
Christopher C. Elisan

Principal Malware Scientist

RSA NetWitness

RSA
FirstWatch

Agenda

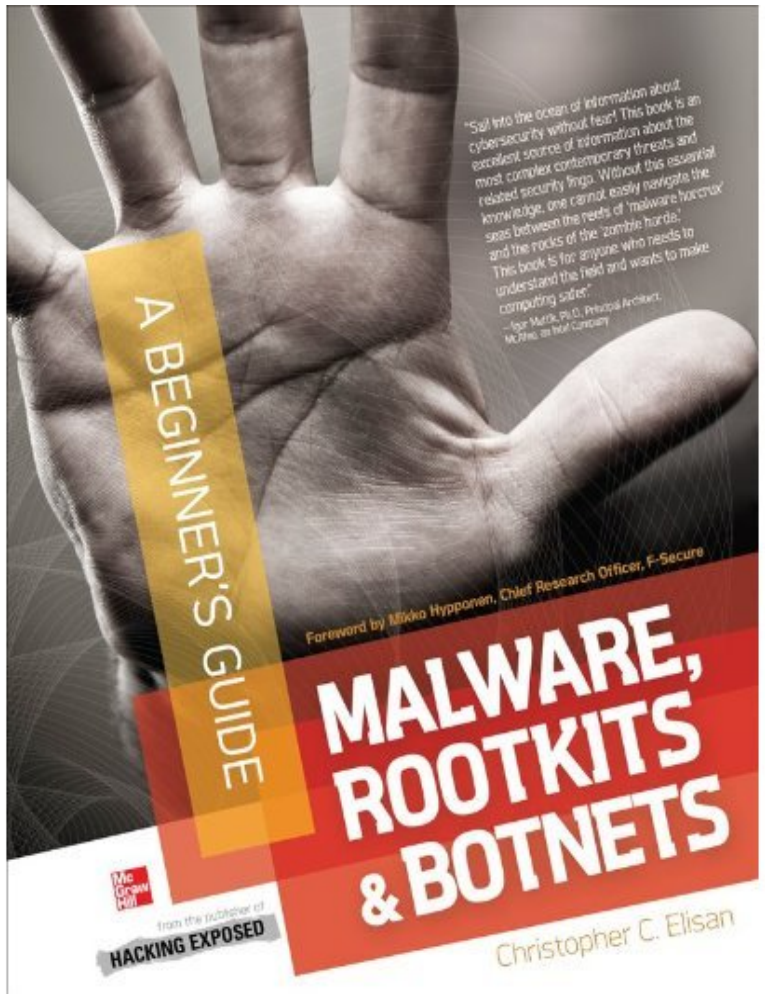


- About Me
- About Us
- VOHO Campaign
- Questions and Answers

RSA FirstWatch

About Me

- Principal Malware Scientist – RSA NetWitness
- Author of *"Malware, Rootkits & Botnets: A Beginner's Guide" (bit.ly/mrbbook)*
- Past Adventures
  - Damballa (2009-2012)
  - F-Secure (2006-2009)
  - Trend Micro (1998-2006
- @Tophs



RSA
FirstWatch

About Us

Advanced Threat Research & Intelligence

- Established in April, 2012
- HQ Reston, Virginia with a Global Scope and Representation
- Heritage dating back to the late 1990s featuring a ‘who’s who’ of researchers
- Elite, highly skilled team focusing on the following areas:
  - Malicious code & content analysis
  - Threat research & ecosystem analysis
  - Automation expertise
- Focused on the threat ecosystem and profiling threat actors
- Mission:
  - To provide RSA NetWitness customers covert tactical and strategic threat intelligence on advanced threats & actors

RSA FirstWatch

Attribution: Who Was Behind VOHO

- Got this question a lot…
- Attribution is difficult:
  - Botnets
  - Registrar / Registry non-cooperation (I'm looking at you ICANN ☺)
  - Anonymization services: TOR, Proxy, VPN
  - DHCP
  - Virtual Machine Images
- We have some very sound ideas…

RSA FirstWatch

VOHO Campaign

- VOHO
  - June / July 2012 by RSA FirstWatch
    - Initially confused with Elderwood (similar MO ‘water holing’; different infrastructure)
    - iSight Partners referred to it as part of the ‘Mourdour’ Trojan campaign
  - Some shared infrastructure
- Multistage Campaign
  - Redirection
    - Heavy dependency on JavaScript on two specific domains for majority of promulgation
- Leverages “Water Hole” technique heavily
  - TOO → TOI → Compromise → Exploitation → Enumeration → Exfiltration → Promulgation

RSA FirstWatch

VOHO Campaign

- VOHO Campaign focused heavily on:
  - Geopolitical targets (especially useful in redirection / promulgation to exploit sites)
  - Defense Industrial Base (DIB)
  - High concentrations of activity noted from a geointelligence perspective in:
    - Boston, Massachusetts
    - Washington, D.C and NOVA
    - Northeastern New Jersey and New York City

RSA FirstWatch

VOHO Campaign

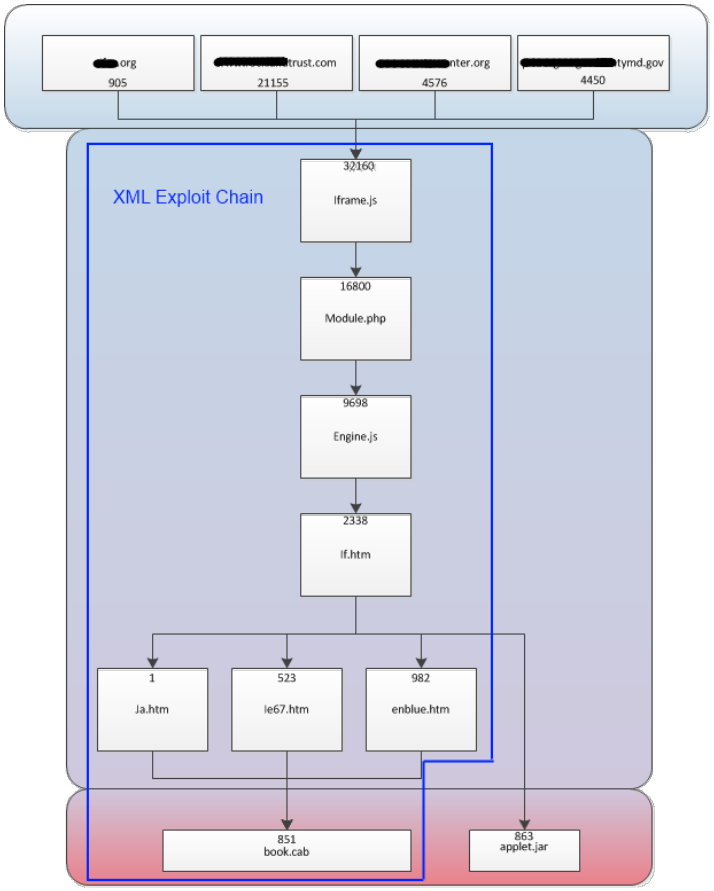
RSA FirstWatch

C2 & Covert Channel Communications Paths

- There were several IP addresses of note in this campaign
- We didn't publish them all in our public paper due to continued research on the campaign and associated campaigns
- Here is a list of C2, Controller Channels, and associates
  - 58.64.155.59 (gh0st RAT C2)
  - 58.64.155.57 (gh0st RAT C2)
  - 58.64.143.245 (gh0st RAT C2)
  - 58.64.158.111 (gh0st RAT C2)
  - 64.26.174.74 (www.torontocurling.com)
  - 134.255.242.47 (VOHO gh0st Controller)
  - 113.10.180.163 (www.goophone.hk)*
  - 113.10.103.170 ("starhub" South Korean broadband)
  - 113.10.113.39 ("starhub" South Korean broadband)

RSA
FirstWatch

VOHO Campaign



Phase I

- *Iframe.js*
  - Iframe.js checks if the visiting machine is running a Windows OS and Internet Explorer. It also sets a cookie value (presumably to track individual visits). If the visiting machine is running a Windows operating system and Internet Explorer, it forward to module.php.
- *Module.php*
  - Module.php uses a simple redirection script to redirect the browser to Engine.js
- *Engine.js*
  - Engine.js looks for processes related to the following antivirus engines using an older vulnerability in Internet Explorer (CVE-2007-4848) that allows local file enumeration.
    - Trend Micro
    - McAfee
    - Symantec

RSA FirstWatch

VOHO Campaign

xKungFoo Script

IE6/7/8 pass kill, I finished writing this POC few days later told foreigners already given POC the above code is our own to explore res agreement was not yet understand, also asked some friends. Now our POC scalability, good, very stable. We can change to change directly.

RSA FirstWatch

VOHO Campaign

- *If.htm*
  - Checks if the visiting host's user agent reflects is one of the following:
    - Unknown
    - Windows XP
    - Windows 2003
    - Windows Vista
    - Windows 7
- Checks if the visiting hosts language settings are:
  - English
  - Chinese
  - French
  - German
  - Japanese
  - Portuguese
  - Korean
  - Russian
- *Enblue.htm*
  - Enblue.htm uses the CVE-2012-1889 XML vulnerability to compromise the visiting browser, which results in a pull and installation of the gh0st RAT malware.
  - This script also appears to be code reuse of a script seen on pastebin as follows:
  - http://pastebin.com/VfmuhEiq
- *Book.cab*
  - Book.cab, the final payload, is an obfuscated executable which, when de-obfuscated using XOR 95, is the gh0st RAT sample named "vptray.exe" (e6b43 c299a9a1f5abd9be2b729e54577)

RSA FirstWatch

VOHO Campaign

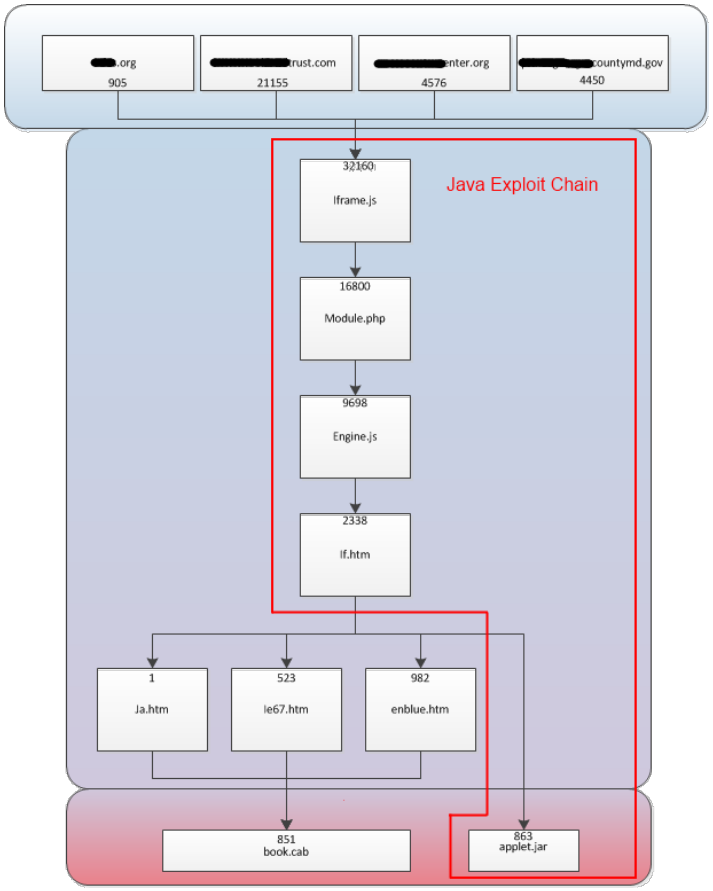
Phase II - Exploit Chain – Sun Java

- Phase II of this campaign was observed July 16-18th, 2012, using the same infrastructure, but with a different directory for the exploit chain files as follows:
  - hxxp://xxxxxxxxxxxxxxcountymd.gov (or other water hole site) → hxxp://www.xxxxxxxcurling.com/Docs/BW06/iframe.js →
  - hxxp://www.xxxxxxxcurling.com/Docs/BW06/module.php →
  - hxxp://www.xxxxxxxcurling.com/Docs/BW06/engine.js →
  - hxxp://www.xxxxxxxcurling.com/Docs/BW06/if.htm →
  - hxxp://www.xxxxxxxcurling.com/Docs/BW06/applet.jar
-

RSA FirstWatch

VOHO Campaign

- *If.htm*
  - In this case, all of the scripts were identical up to “if.htm”, which instead contained a java call that loaded applet.jar, as well as a large blob of obfuscated code as a “param” element. This large blob of code is a binary obfuscated with XOR 77, which the java applet deobfuscates and runs as “svohost.exe” (2fe340fe2574ae540bd98bd9af8ec67d).



RSA FirstWatch

The VOHO Malware Families

- Fake Symantec Update
- Fake Microsoft Update

RSA FirstWatch

Fake Symantec Update

- VPTray.EXE
- UPX compressed binary
- Local Settings\Temp folder
- Autostart
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Run
  - HKEY_USERS\<User's Security ID>\Software\Microsoft\Windows\Current\Version\Run
  - Value = SymantecUpdate
  - Data = 43:3a:5c:44:4f:43:55:4d:45:7e:31:5c:41:44:4d:49:4e:49:7e:31:5c:4c:4f:43:41:4c:53:7e:31:5c:54:65:6d:70:5c:56:50:54:72:61:79:2e:65:78:65:00
    - C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\VPTray.exe
- Protective Mechanisms
  - Registry Editor is disabled
  - Windows System Restore is disabled

RSA
FirstWatch

Fake Microsoft Update

- SVOHOST.EXE
- UPX compressed binary
- Local Settings\Temp folder
- Autostart
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Run
  - HKEY_USERS\<User's Security ID>\Software\Microsoft\Windows\Current\Version\Run
  - Value = Microsoft Update
  - Data = 43:3a:5c:44:4f:43:55:4d:45:7e:31:5c:41:44:4d:49:4e:49:7e:31:5c:4c:4f:43:41:4c:53:7e:31:5c:54:65:6d:70:5c:73:76:6f:68:6f:73:74:2e:65:78:65:00.
    - C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\svohost.exe
- Protective Mechanisms
  - Registry Editor is disabled
  - Windows System Restore is disabled

RSA
FirstWatch

Victim Notification

RSA
FirstWatch

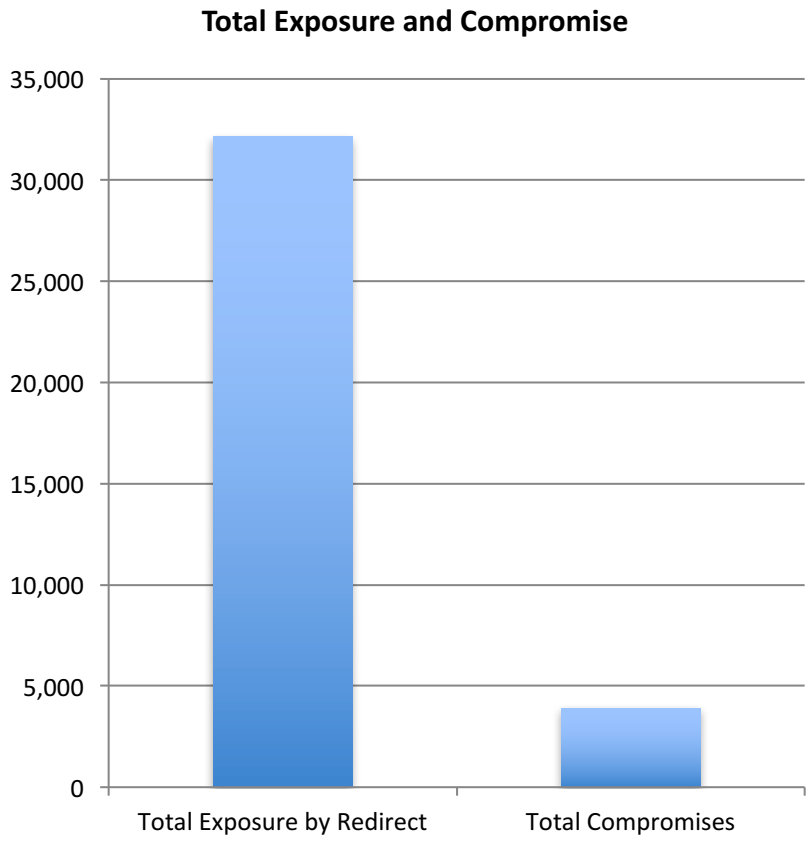
Victim Notification

- Endeavored to notify victims -- ~1000
- Response
  - None
  - Anger / Fear / **Panic** / Frustration
  - Curiosity
  - Sense of Urgency
- LE Response
  - Wished we'd notified them first as they felt our research caused some parties to 'panic'
- Altruistic intent; no sales pitch

RSA FirstWatch

VOHO Campaign

The Trooper



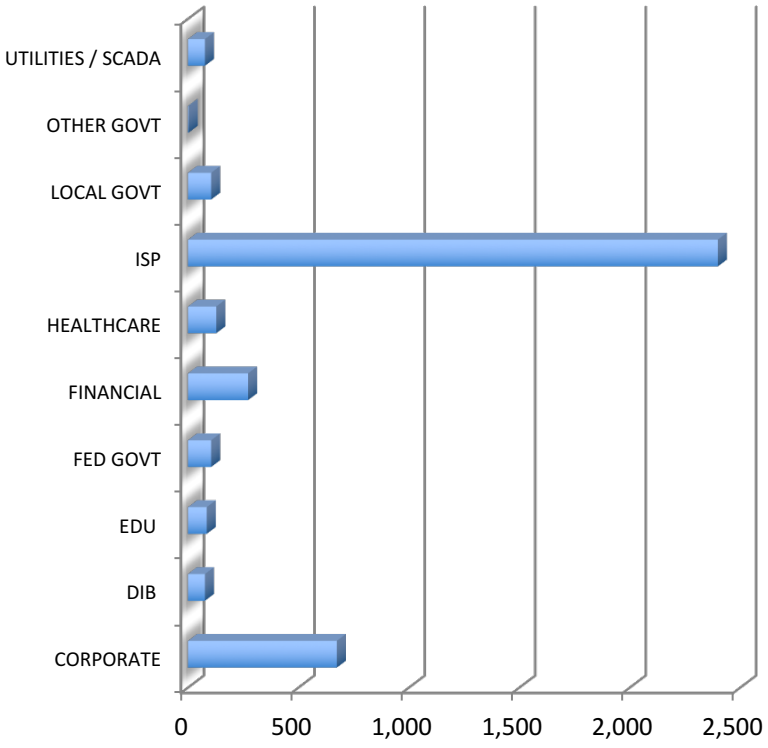
- Total of 32,160 unique hosts
- Representing 731 unique global organizations
- Redirected from compromised web servers injected with the redirect iframe to the exploit server
- Of these redirects, 3,934 hosts or 12% were seen to download the exploit CAB and JAR files (indicating a successful exploit/compromise of the visiting host)
- Based on our previous understanding of exploit campaigns, indicates a very successful campaign.

RSA FirstWatch

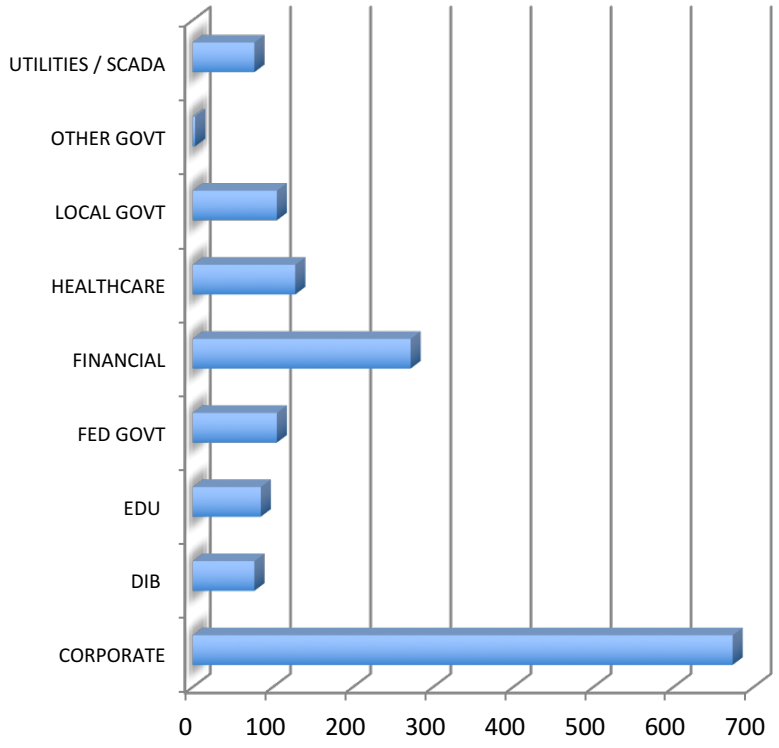
VOHO Campaign

The Trooper

Compromises by Industry

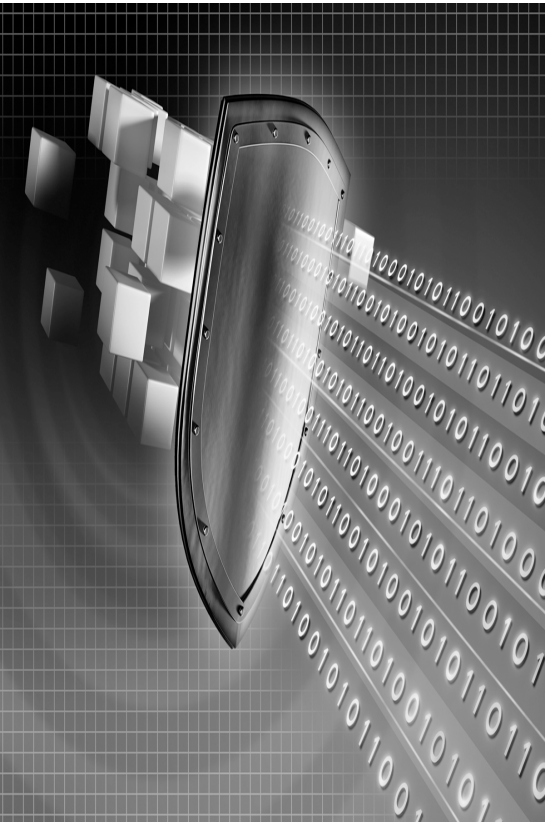


Compromise By Industry (without ISP)



RSA
FirstWatch

The VOHO Campaign Paper



Authors:

Will Gragido, Sr. Manager RSA First Watch
Chris 'Tophs' Elisan, Principal Malware Scientist RSA First Watch
Jon McNeil, Principal Threat Researcher RSA First Watch
Alex Cox, Principal Threat Researcher RSA First Watch
Chris Harrington, Threat Researcher, EMC CIRC

RSA
FirstWatch

THANK YOU