



Microsoft, the CIA and NSA Collude to Take Over the Internet

Wednesday, June 20, 2012

Contributed By:

Jesus Oquendo



Clever security researchers have uncovered the biggest security Coup d'état on the planet.

Microsoft, the NSA, the CIA have all been colluding to create the most **bloated** covert piece of malware known to exist for 5 years [1] undetected. Microsoft decided somewhere along 2006 and 2007, that it was willing to throw away half of their market share (128 billion) in allowing this to occur [2].

Let us begin to analyze how this occurred. Obviously the NSA, CIA and others involved had to determine a mechanism to get the right talent hired at Microsoft. Not a big deal, the NSA has some very talented individuals.

Once hired, they had to make sure that the injected individual be placed in the EXACT department responsible for certain elements of the Windows operating system. Once that was done, the agencies had to then bypass any kind of code versioning system MS [Microsoft] had in place that should have detected code changes.

In most software environments, that would mean quiet possibly hundreds of programmers who would have seen those changes. Because they are the NSA and CIA however, they pulled it off.

They managed to bypass Microsoft's HR [Human Resource] filters, bypass software developers who would have noticed changes in code, managed to get it to the market, then managed to ensure that ONLY certain countries would get the tainted OS environment.

Priceless. Reminds me of some Oceans Eleven style event.

Let us think about another method here. The CIA, NSA and Microsoft decided to pull this off. They created a completely separate operating system somewhere in the Beltway. Microsoft decided to give the agencies the specific code to make the rogue changes.

After those changes were made, Microsoft made an executive decision to allow the rogue system to be placed inside of their network and only allow a specific country to be infected by this. Surely that is how it went down. Microsoft had to make



sure that all employees who noticed this anomaly would keep it a secret. Including all of their non-US citizen employees.

To do so, they offered extensions on their H1B Visas. All was kept secret for years, obviously. Pick your poison here, Let me know which sounds more absurd.

When it comes to "big brother" based intervention, circumvention or any other type of scenario, I am usually all over it. I have been this way since that days of Carnivore [3], CIPAV[4], and a slew of other articles pointing out instances where **big brother seemed to have their hands in the cookie jar.**

Certainly I am no stranger to seeing, reading, or hearing about oddities however, this particular theory that the NSA, CIA and or some other covert agency infiltrated Microsoft to pull this off is outright laughable. I don't even think laughable is the right term however, it just fits.

So there you have it. Had to be the NSA, CIA and other operatives quite simply because it fits. Forget the fact that someone was trying to sell a book when they reported: "Obama said, should we kill this thing" (referring to Stuxnet). We are to believe that the author had firsthand knowledge and an account of what went on in a secret meeting. Don't question this now children! Just believe! Or, we are to believe the: "I could tell you but then I would have to..." theory.

So many people are blurring the lines with technology and politics it is scary. Scary in the sense that too many assumptions are being made based on information that comes out of the sky. Anyone can create these types of malware, this is not a secret.

Many of the organized crime groups have the same capabilities as the authors of Flame and Stuxnet. In fact, many organized crime organizations have better techniques, tactics and tools than Flame. They have the money, means and motives to pull these same tactics off. In fact, they could likely pull it off more covertly.

Nevertheless, it is fun, hip and groovy to throw these theories out. With that said, here is a theory that was posted on Pastebin. I call it "False Flag Cyber Joe Jobbing" however the author dubbed it: "Internet and Oil Markets going to Flame(s)":

- Original <http://pastebin.com/8KkA7hk3>

Internet and oil markets going to Flame(s)

*Russia and China may now be framing the United States and other countries using cyberwarfare tactics. This should not be a startling statement nor should anyone brush this statement off as hearsay. In order to understand the dynamics of this theme, you the reader need to be aware of **global politics, computing and a bit of intelligence.***

I will begin with Kaspersky as an individual followed by the company. Yevgeniy (Eugene) Kaspersky is a graduate of the Russian FSB's IKSI. IKSI is the Institute of Cryptography, Telecommunications and Computer Science of the FSB Academy. [FSB] Kaspersky you may recall wants an end to freedom on the Internet: "I'd like to change the design of the Internet by introducing regulation ... about following Internet standards. And if some countries don't agree with or don't pay attention to the agreement, just cut them off." [ZDN] Do you need a translation of what Kaspersky was aiming for? If so, this write up is not for you.

Fast forward to almost three years following that statement. Surprise! Kasperky discovers "the most complex malware ever produced." No one has ever seen nor heard of it. Granted there are hundreds of millions of users in the world and hundreds of antivirus companies around. How many hundreds of thousands of security researchers? Yet according to Kaspersky and company, this "Flame" malware has been around for years without ever being detected. What is the saying? If it sounds too good to be true?

Often times, I am asked as a security professional: "Don't you think that the antivirus companies launch these things to scare us into buying their products." Often my response is: "Why should they, there are enough criminals attacking operating systems. The AV companies won't have to." Whereas now, things are starting to make a little more sense. Did Kaspersky create a strain to rattle global politics? Why couldn't he do so. After all, he is in some capacity FSB. If you recall, Kaspersky's son was kidnapped and held for some ransom, what is to stop him from being blackmailed by the FSB of all agencies into making something like Flame. It would make logical sense.

Flame is known for targeting only Middle East targets. Mainly oil companies. Coincidentally, Russia has also been on a rampage when it comes to oil, after all it all boils down to money at the end of the day. [OIL] So why is everyone hell-bent on trying to connect the dots associated with Flame and the United States. It could quite possibly entail nothing more than a power play for Russia to attempt to gain a certain amount of control of the Internet. This allows them to be able to determine dissidents via way of Internet taps. It also gives them a greater stage to collaborate and earn Chinese currency.

Granted, Flame would have to be state sponsored, as a kid there was a running theme that "whomever smelt it dealt it." This is likely to be the case. State sponsored indeed. What better way to light fire to the United States than it would be to shift the blame on the country via a horribly written, bloated piece of malware. You know that same piece of malware that has five different encryption mechanism. Psssttt... Mr. Kaspersky, didn't you graduate crypto school? China, your role will be analyzed soon however, it need not take a global political science major who doubles in forensics to connect those dots.

Veritas vos liberabit

*R/
Immanuel Hume*

[FSB] http://en.wikipedia.org/wiki/Institute_of_Cryptography,_Telecommunications_and_Computer_Science

Yea, that's the ticket.

Sources:

[1] <https://www.prevx.com/filenames/2285400525247160256-X1/WAVESUP3.DRV.html>

[2] <http://www.federalnewsradio.com/241/2911172/NSA-CIA-helped-Israel-develop-flame-computer-virus>

[3] <https://www.google.com/search?q=circumventing+carnivore>

[4] <https://www.google.com/search?q=cipav+infiltrated>

Cross-posted from [Infiltrated](#)

J Oquendo

Breaker of the Unbreakable

Summary

Security professional working in the Northeast. I wear multiple hats, red (penetration testing), green (DFIR) and blue (defense). I no longer publicly disclose the companies I work for - but feel free to ask.

Specialties: Pentesting, DFIR, net forensics (packet fun), system forensics, mobile forensics. Covert Network Attacks, Covert Network Exploitation, Information Assurance, Information Operations, Threat Analytics.

Security Research with exploitable discoveries on IBM, Microsoft, Cisco, F5, VMWare, SAP, Adtran, etc.

Experience

Infrastructure Demolition Engineer at Essexotec

June 2014 - Present

Analysis of the (sometimes) unbreakable: networks, applications, frameworks, and threat intelligence. I break things, sometimes I even fix them. Job duties consist of uncommon penetration testing (who needs tools), vulnerability assessments, risk analysis, threat analysis, risk/threat mitigation, and a whole slew of other security buzzwords. Incident response and forensics. Well versed in drinking coffee

Lead Security Engineer

December 2011 - June 2014 (2 years 6 months)

Lead Security Engineer responsible for managed security services and product development. Penetration Testing (Red Team), Risk Assessments, Mobile and Data Forensics.

Advanced Persistent Security Threat at Cyber Security Forum Initiative

November 2011 - June 2014 (2 years 7 months)

Developing core content on advanced penetration testing (covert channels, encryption, stego), forensics, counter-forensics and counter-counter-forensics concepts, techniques, theories and approaches. Teach concepts to cleared candidates via CNA and CNE courses.

Senior Security Engineer at IPC Systems, Inc.

November 2011 - December 2011 (1 month)

Senior Security Engineer at an undisclosed company with a focus on increasing the security of company's products. Partially developed a security strategy for security test cases in an effort to map security processes, guidelines and frameworks to ensure quality security for company's clients.

Collaborated with various departments in an effort to achieve a solid "security-centric" SDLC which was to provide focused, clear, concise, repeatable, transparent and measurable security objectives while exceeding common security baselines.

Developed new, and revised existing security test cases while mapping frameworks, guidelines, regulatory controls into a uniform structure to minimize risk.

Senior Security Flunky

June 2006 - November 2011 (5 years 5 months)

Lead Security Engineer responsible for security services and product development. Penetration Testing (Red Team), Risk{Analysis,Assessments,Management} Security product deployments, hardening, management and configuration (FW, IPS/IDS/ITS). Infosec threat analysis, compliance auditing and defensive countermeasures on enterprise networks. Security Incidence Response and Forensics. Developed proprietary penetration testing processes. Developing proprietary SIEM based on Open Source tools framework, Security information awareness training... VoIP Engineering (analysis, security, development and deployment) and too many other tasks I squeeze into the day

Environment: Cisco, Foundry, Juniper (ESX), Netrake nCite Session Border Controllers, LDAP, Checkpoint FW-1, Netscreen (Starbucks!), Sonicwall, Stonesoft Stonegates, Asterisk, ISA Server, Cacti (Starbucks!), Rancid, MRTG, OSSIM, ZenOSS, Raritan CommandCenter NOC, etc. (Starbucks!)

Senior Systems Engineer and Network Administrator

January 2004 - March 2006 (2 years 2 months)

Senior systems and network administrator. Administration for 3 remote offices using VPN's, KVMoIP. Checkpoint, Netscreen and Windows SMB 2003 administration. Designed and implemented a VoIP infrastructure between 2 locations and was working on a third using Cisco switches, routers and phones. Created and implemented an MS Project-like system based on LAMP Re-designed infrastructure and deployed an entirely new infrastructure that maximized uptime and reduced costs. Implemented security and user policies throughout. Daily Cisco and Adtran router administration. Oracle 11g database design and implementation for HR administrative tasks. Environment: Nokia, Checkpoint Firewall-1 and VPN-1, Safe@Office, OpenBSD Packet Filter and VPN (isakmpd), PGP, Netscreen, Snort, Network Flight Recorder Sentivist, Sun Fire v280R, Oracle, PHP, Linux (CentOS) administration, Windows SMB2003, MS Exchange, SuSE OpenExchange, OpenOffice, Veritas Backup Manager, Apache-SSL, Oracle 11g, S/MIME

Network/Security Engineer

July 2003 - December 2004 (1 year 5 months)

Systems and Network Administrator (40 FreeBSD hosts). Administration of ADSL/SDSL/T1/T3 based network configurations. Disaster Recovery, Apache (1500+ domains/15000+ users) Postfix/Courier IMAP/POP, MySQL, DHCP server for 2000+ DSL customers. Wrote custom expect scripts for extracting route cache from routers to identify and track Denial of Service attacks. Built custom router/firewall for office

network transitioning from static IPs to a NAT setup with vlans and rate limits. Installed and supported an ISP infrastructure including servers, storage, operating systems, infrastructure in an ISP-serving CLEC network. Configured Cisco routers and switches for both customers and use in the core network. University work: IT administrator for RESNET. Cabling of dormitories, configuration, and administration of campus' OC3 and six T1 connections. Environment: Checkpoint, BSD (PF) and VPN (isakmpd), IPFilter, SunScreen 3.x, Pix, Snort, Sun Fire 4800, E 6000/6500, Netra T1, HP A, class servers

Security Engineer

1999 - 2000 (1 year)

Education

SANS

Reverse Engineering Malware (GREM), 2011 - 2011

Long Island University


1998 - 2001







J Oquendo

Breaker of the Unbreakable



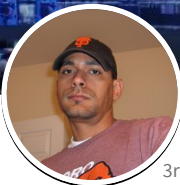
[Contact J on LinkedIn](#)





Try Premium for Free

Node.js MongoDB Developer - Cincinnati-based software developer available for contract work. | Ad




3rd

J Oquendo

Breaker of the Unbreakable

Essextec • SANS

Hartford, Connecticut Area • 500+ 

Send InMail

Connect

Security professional working in the Northeast. I wear multiple hats, red (penetration testing), green (DFIR) and blue (defense). I no longer publicly disclose the companies I work for - but feel free to ask.

Specialties: Pentesting, DFIR, net forensics (packet fun), system forensics, mobile forensics. Covert Network Attacks, Covert Network Exploitation, Information Assurance, Information Operations, Threat Analytics.


Security Research with exploitable discoveries on IBM, Microsoft, Cisco, F5, VMWare, SAP, Adtran, etc. [See less](#)

Contact and Personal Info

J'S Profile

[Show more](#)

The difference between a smart idea and a story




Avnet guides you from idea to mar

Learn More

J'S Articles & Activity


955 followers



Technical Thoughts and Comments on the Cyber...


J Oquendo on LinkedIn

February 24, 2017




Listen up. I don't care how many friends, or former employers, or skill areas, we have in...

J replied to a comment



Why don t you see hackers hiding in their parent's basements anymore? Because they...

J commented




Getting ready to talk about Baldrige Cybersecurity Excellence Builder at the 29th...

J liked

See 36 more articles

See all activity

Experience




Infrastructure Demolition Engineer

Essextec

Jun 2014 – Present • 2 yrs 11 mos

Analysis of the (sometimes) unbreakable: networks, applications, frameworks, and threat intelligence. I break things, sometimes I even fix them. Job duties consist of uncommon penetration testing (who needs tools), vulnerability assessments, risk analysis, threat analysis, risk/threat mitigation, and a whole slew of other security buzzwords. Incident response and forensics. Well versed in drinking coffee


[See less](#)



Lead Security Engineer

E-Fensive Security Strategies


People Also Viewed



Shannon Rose • 3rd

Owner, The Telephone Connect


[Connect](#)



Matt Galin (CISSP, GIAC-MultiP.

Sr. Security Analyst at Hartford Services Group


[Connect](#)



Lance Miller • 3rd

The Cetan Group, Managing Par


[Connect](#)



Scot A Terban

Cyber Nihilist


[Connect](#)



Rob Fuller • 3rd

Infosec Treehugger


[Connect](#)



Michael Serrine • 3rd

Cyber Security Analyst at Holyo Electric


[Connect](#)



Marcus Carey • 3rd

Founder & CEO at vThreat




[Connect](#)



Fabienne Serriere


CEO of KnitYak LLC







[Connect](#)


Messaging   


<https://www.linkedin.com/in/efensive/>



1/3










 Try Premium for Free

[See description](#) 

**Advanced Persistent Security Threat**
Cyber Security Forum Initiative
Nov 2011 – Jun 2014 • 2 yrs 8 mos
Cyber Security Forum Initiative - CyberWarfare Division
[See description](#) 


**Senior Security Engineer**
IPC Systems, Inc.
Nov 2011 – Dec 2011 • 2 mos
Fairfield, Connecticut
[See description](#) 

**Senior Security Flunky**
E-Fensive Security Strategies
Jun 2006 – Nov 2011 • 5 yrs 6 mos
[See description](#) 

[See more positions](#) 

Education

SANS
Reverse Engineering Malware (GREM)
2011 – 2011

Reverse-engineering malicious applications, scripts and applets
Reverse-engineering and analyzing malicious Microsoft Office (Word, Excel, PowerPoint) and Adobe PDF documents
Examining shellcode in the context of malicious files
Analyzing memory to assess malware characteristics and reconstruct infection artifacts
Memory forensics to analyze rootkit infections
[See less](#) 

Long Island University
1998 – 2001