LATERAL | SECURITY

INFORMATION SECURITY SPECIALISTS

# *Combating APT with SRP*


Presenter: Tim Thomson

Date: October 2011

Company: Lateral Security (IT) Services Limited


LATERAL | SECURITY

# Agenda

- APT + demo
- Application Whitelisting
- Software Restriction Policies
  - Configuration + demo
  - Operation + demo
  - Bypassing + demo
- Questions

# APT

- Nation State
- 0-day
- Patient
- Targeted
  - AV won't help

# Modus Operandi

- Emailed malicious documents
  - Targeted, relevant topic
  - Often spoofed from a frequent contact
  - Often resend of legitimate documents
- USB keys
  - Police Computer??

The Telegraph

Mossad spy ring 'unearthed because of Christchurch earthquake'

The Israeli secret service Mossad has been accused of conducting an intelligence-gathering operation in New Zealand which was unearthed because of February's Christchurch earthquake.

Cars lie under rubble in the central business district in Christchurch Photo: AFP/GETTY IMAGES

# Aurora


## A new approach to China

1/12/2010 03:00:00 PM

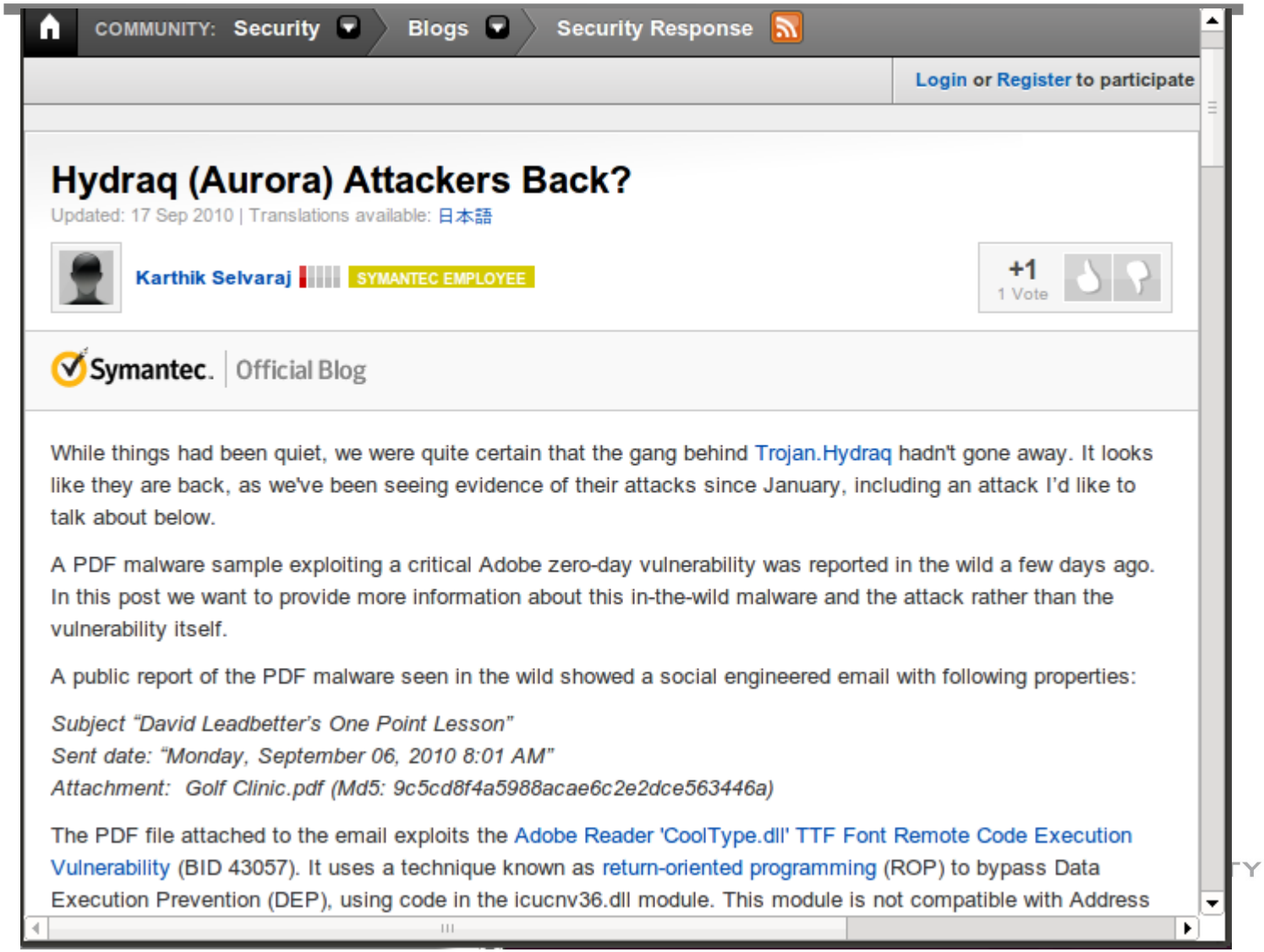
Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves.

Third, as part of this investigation but independent of the attack on Google, we have discovered that the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers.

# Aurora



COMMUNITY: Security | Blogs | Security Response

Login or Register to participate

## Hydraq (Aurora) Attackers Back?

Updated: 17 Sep 2010 | Translations available: 日本語

Karthik Selvaraj SYMANTEC EMPLOYEE

+1
1 Vote

Symantec. | Official Blog

While things had been quiet, we were quite certain that the gang behind Trojan.Hydraq hadn't gone away. It looks like they are back, as we've been seeing evidence of their attacks since January, including an attack I'd like to talk about below.

A PDF malware sample exploiting a critical Adobe zero-day vulnerability was reported in the wild a few days ago. In this post we want to provide more information about this in-the-wild malware and the attack rather than the vulnerability itself.

A public report of the PDF malware seen in the wild showed a social engineered email with following properties:

*Subject "David Leadbetter's One Point Lesson"*
*Sent date: "Monday, September 06, 2010 8:01 AM"*
*Attachment: Golf Clinic.pdf (Md5: 9c5cd8f4a5988acae6c2e2dce563446a)*

The PDF file attached to the email exploits the Adobe Reader 'CoolType.dll' TTF Font Remote Code Execution Vulnerability (BID 43057). It uses a technique known as return-oriented programming (ROP) to bypass Data Execution Prevention (DEP), using code in the icucnv36.dll module. This module is not compatible with Address

# Agent.btz

## Under Worm Assault, Military Bans Disks, USB Drives

By Noah Shachtman ✉ November 19, 2008 | 3:12 pm | Categories: Info War

The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further.

The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret SIPR and unclassified NIPR nets. The suspension, which includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately." Similar notices went out to the other military services.

In some organizations, the ban would be only a minor inconvenience. But the military relies heavily on such drives to store information. Bandwidth is often scarce out in the field. Networks are often considered unreliable. Takeaway storage is used constantly as a substitute.

The problem, according to a second Army e-mail, was prompted by a "virus called Agent.btz." That's a variation of the "SillyFDC" worm, which spreads by copying itself to thumb drives and the like. When that drive or disk is plugged into a second computer, the worm replicates itself again — this time on the PC. "From there, it automatically downloads code from another location. And that code could be pretty much

# Old worm won't die after 2008 attack on military

Thu, Jun 16 2011

By Phil Stewart and Jim Wolf


WASHINGTON (Reuters) - Three years after what the Pentagon called the most significant breach of U.S. military networks ever, new versions of the malware blamed for the attack are still roiling U.S. networks, Reuters has learned.

The malware at issue, known as "agent.btz," in 2008 infiltrated the computer systems of U.S. Central Command, which was running the wars in Iraq and Afghanistan.

The attack established what Deputy Defense Secretary William Lynn called "a digital beachhead" for a foreign intelligence agency to attempt to steal data.

The Pentagon last year disclosed its operation to counter that attack, known as Buckshot Yankee. But new, more potent variations of agent.btz are still appearing.

"We can definitely say that it's not limited to government computers, it never has been, and that it hasn't gone away," said an official of the Department of Homeland Security, which leads U.S. efforts to secure federal nonmilitary computer networks, often described as the Internet's "dot.gov" domain.

"It's very persistent and it keeps evolving," the official said. "You're constantly seeing new, better versions of it. So it's a challenge to keep ahead of it."

"It's quite prolific," the official added, speaking on condition of anonymity because of the matter's sensitivity. The official did not specify precisely which networks have been affected or the extent of the damage.

FOREIGN SPY AGENCY

U.S. officials have said a foreign spy agency was responsible for the 2008 attack, which occurred when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East.

But they have never publicly named which one. Reuters has learned that experts inside and outside of the U.S. government strongly suspect that the original attack was crafted by Russian intelligence.

Information about the origin of the suspected attackers, however, is still closely held and Pentagon officials refuse to

# Agent.btz

- Hit US Military in 2008
- Air-gap jumping C2
- Extended clean-up operation
- Resulted in US Cyber Command
- Russians?
- Still there!

# Stuxnet

- Highly targeted payload
- Iranian uranium enrichment
- Four 0-day exploits
- Israel/US?

# Malware Demo

LATERAL | SECURITY

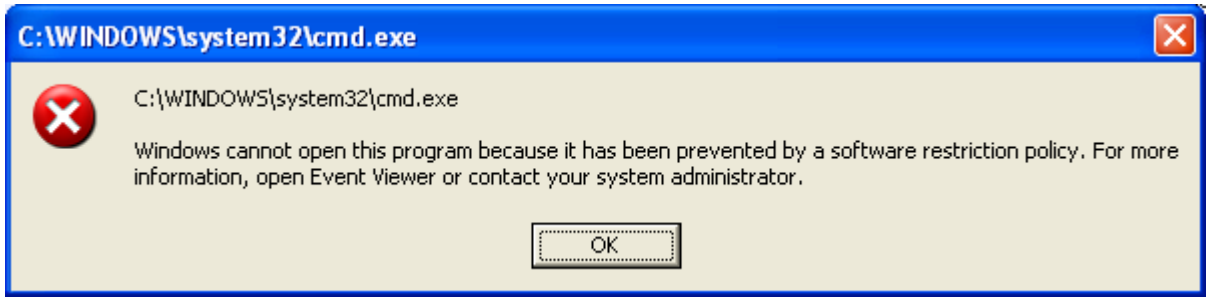
# Application Whitelisting

- Blacklisting?
  - Enumerate *all* the bad in the world?
- List what you need to do your job
- Don't just stop install: Block execution
- Many commercial solutions
  - AppLocker
- #4 in DSD's Top 35 Mitigations

LATERAL | SECURITY

# Software Restriction Policies

- Available since XP
- Commonly used for blacklisting




  - Trivial to bypass in this mode
- Only effective in whitelisting mode

# Basic Concept

- Allow paths with software, e.g.:
  - c:\windows
  - c:\program files
- Ensure user can't write there
  - Sysinternal's Accesschk
- Set default to “Disallowed”
- Everything else is blocked by default

# Implementation

- Deployable from Group Policy
- Check user write permissions
  - Sysinternal's accesschk
  - Remove write access to allowed paths
  - Or add writeable paths to blacklist

# Implementation cont

- Create New Software Restriction Policy
  - Include DLLs
  - Remove .lnk files?
  - Set default rule to disallowed
- Deploy to test group
- Deploy across domain

# Implementation - Logging

- Existing environments: enable additional logging pre-deployment
- Leave in unrestricted mode for logging
- Set `HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\LogFileName`
- Deploy to test group
- Watch for default rule hits

# Config Demo

# Issues

- Doesn't block initial exploit, or shellcode
- User mode protection only
- No per-user rules
- Crap GUI
- No network service protection

# Bypasses

- Shellcode execute exe/dll:
  - LoadLibraryEx flag LOAD_IGNORE_CODE_AUTHZ_LEVEL
  - CreateRestrictedToken/CreateProcessAsUser flag SANDBOX_INERT
- runas /trustlevel:unrestricted
- rundll if not restricting DLLs
- gpdisable if admin

# … but still effective!

- Most shellcode doesn't attempt bypass
- Many vulnerabilities don't use shellcode
- Stops USB autorun style malware
- Breaks persistence after logoff/reboot
- Can provide additional logging for IR

# Prerequisites

- Not admin (#3/35)
- Enable DEP (#20/35)
- Disable Macros (#26/35)
- Firewall (#13 & #14/35)

# SRP Demo

# Conclusion

# Conclusion

It's crap

# Conclusion

BUT

LATERAL | SECURITY

# Conclusion

- It stops latest APT:
  - “Chinese”
  - “Russian”
  - “USA/Israel”
  - Lots of normal malware

LATERAL | SECURITY

# Conclusion

- Good first step
- Relatively easy
- Already built in
- Turn it on

# Further Reading

- http://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf
- http://dsd.gov.au/infosec/top35mitigationstrategies.htm
- Samples from:
  - http://contagiodump.blogspot.com/
  - http://offensivecomputing.net

LATERAL | SECURITY

# Questions?

Thank you

Lateral Security (IT) Services Limited
38-42 Waring Taylor Street
PO Box 8093, Wellington 6143, New Zealand

Phone: +64 4 4999756
Presenter: tim.thomson@lateralsecurity.com
Web: https://www.lateralsecurity.com

LATERAL | SECURITY