



The New Frontier: Cyber Attack Vectors

December 8, 2011

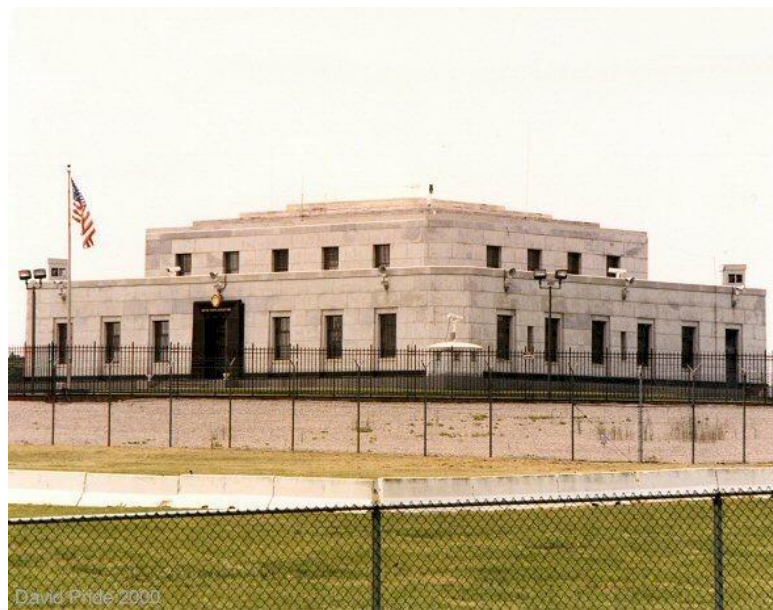


Yesterday's Security Approach: P4

- Perimeter Protection, Patch & Pray
 - (borrowed from DARPA PM Howard Shrobe)

Security used to be based on strong perimeters. All of the “good things” were inside and all of the “bad things” were outside.

Today neither of these is true.



The Threat in the News

“Maneuvering in Cyberspace” was the name of September’s conference in Lithicum, Maryland.

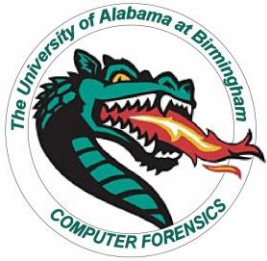
General Alexander told the assembled Department of Defense and Academic Researchers that the level of intrusion into DOD networks is higher than ever.

“Cyber threats represent a problem on a massive scale that affects every industry and sector of the economy and government”



General Keith Alexander,
Director of US Cyber
Command at Fort Meade

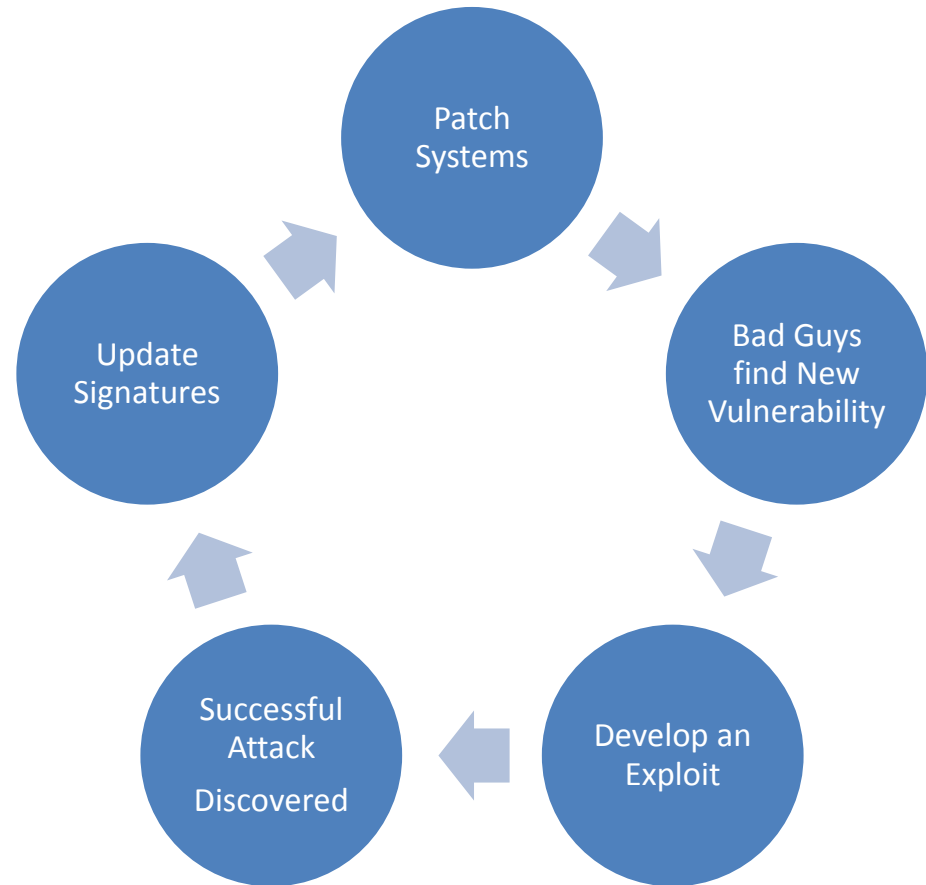
“Alexander Cites Need for Greater Cyber Defenses” -- <http://www.defense.gov/news/newsarticle.aspx?id=65321>



The security cycle

The current process, described by General Alexander at last month's DARPA Cyber Colloquium doesn't work.

We need a Defensible Architecture



The Threat in the News

This fall the “Summit on Advanced Persistent Threats” was held in Washington DC. One hundred Chief Information Officers and Chief Information Security Officers met with RSA Security Chief Eddie Schwartz to discuss the threats to their organizations from having their networks infiltrated.

“The frequency and volume of attacks have reached pandemic levels,” Schwartz cautioned the attendees.

Organizations have all conducted some form of employee training or awareness programs, but the traditional programs were generally perceived as being a waste of money

<http://www.eweek.com/c/a/Security/Executives-Discussed-Security-Breaches-Attacks-During-APT-Summit-296714/>



RSA Security Breach lead to intrusions at Lockheed Martin

The cost to RSA > \$100M

Email-Based Attacks

What have some of the biggest cyber attacks of the year, including the RSA breach, multiple DOD breaches, the Google “Operation Aurora” case, the HBGary hack, “Operation Night Dragon”, “Operation Shady RAT”, GhostNet, and other breaches all have in common?

They started with an email

Email Security

Protecting Corporate Email is challenging.

Your greater email threat is the one that passes straight through your Perimeter.

Individuals checking their Gmail, Yahoo, Hotmail, AOL, and personal emails ...

And their online forum messages at SportsFans.com, and RussianBrides.com, and AllNaturalBodyBuilders.com ...

Who scans the attachments and links on those sites?



“Spear Phishing”

The RSA breach started with an email received by four EMC employees – sent to one and cc’ed to three others.

Subject: 2011 Recruitment Plan

I forward this file to you for review.

Please open it and view it.

Attachment: 2011-Recruitment.xlsx

Dangerous spreadsheets?

If the Excel file was opened, and it has been confirmed that it was, a “Flash” object in cell A1 was executed.

That object contained code that caused the computer that viewed the file to connect to “good.mincesur.com” a hacked computer in Korea, and download a Remote Administration Trojan called “Poison Ivy”.

It installed itself as a file called “Expl0rer.exe” (with a zero instead of the letter “o”).



Some of the features of "Poison Ivy":

- File search*
- File transfer*
- Registry Edit*
- Registry Search*
- Password hash dump*
- Network capture*
- Screen capture*
- record audio*
- record camera*

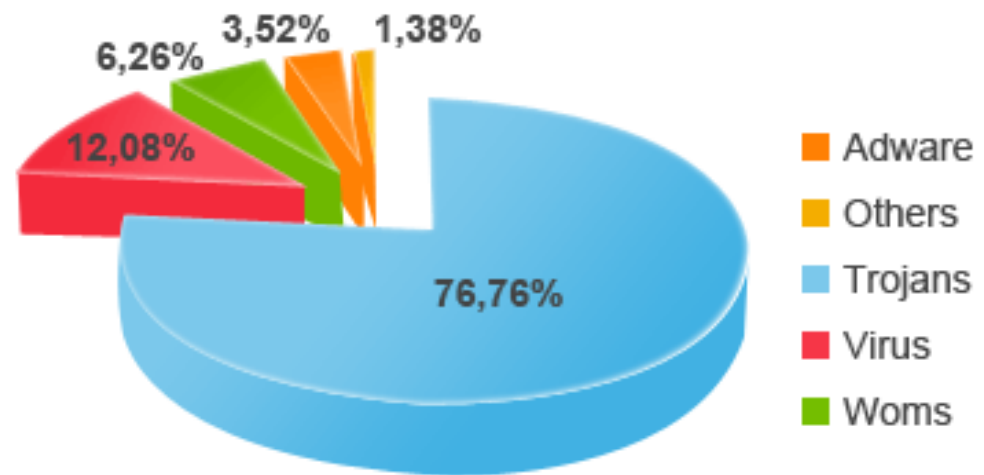
And many more . . .



5 million unique malware samples in 2011Q3

"The highlight of the third quarter is the record set in the creation of new Trojan samples," said Luis Corrons, Technical Director at PandaLabs. **"Three out of four new malware samples created by cybercriminals are Trojans**, creating further proof that their sole intent is to steal users' information."

Infiltration of systems for future exploitation is the current top malware development priority!





Yesterday's Email Threats

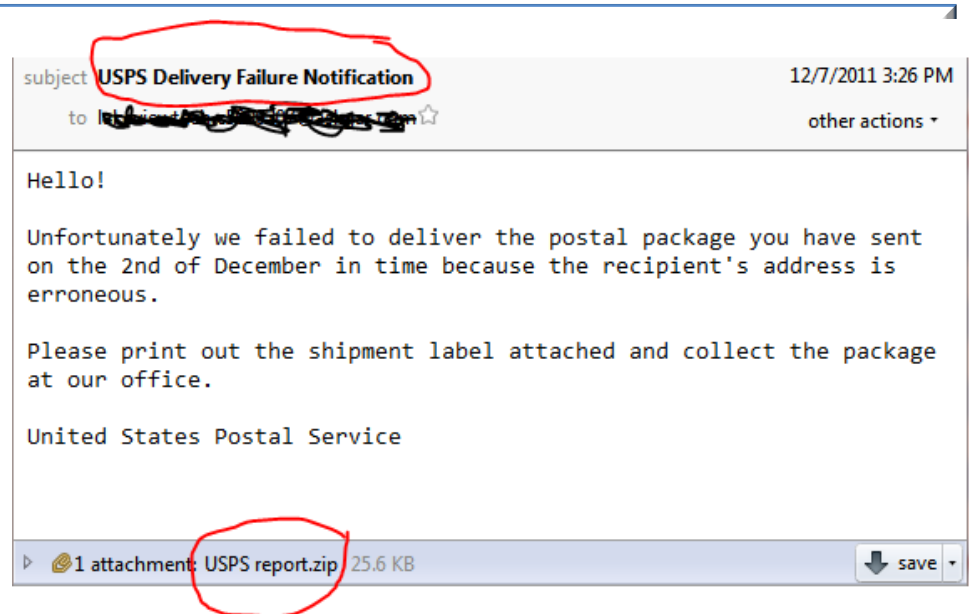
Here are some of the top email subjects that we received yesterday in the UAB Spam Data Mine that can be “malicious”

| | |
|---|--|
| 14313 USPS Delivery Failure Notification | 1189 AARP Discounts Notice |
| 6530 Increase your fortune now | 1102 Re: got those pics for you |
| 2060 Fwd: Order confirmation | 796 Up to 1500 USD in 1 hour |
| 2019 Fwd: Re: Order confirmation | 758 Struggling this holiday season? |
| 1891 Bad Credit OK - Up to 1500 | 751 BBB Complaint activity report |
| 1535 FDIC: About your business account | 748 Complaint from your customers |
| 1499 Insurance of your business accounts | 713 ACH transaction report |
| 1474 FDIC: Your business account | 711 Yulenska wants to be your friend |
| 1464 FDIC: About your business accounts | 708 Regions - Message |
| 1443 Insurance coverage of your business accounts | 685 CRITICAL: There has been a change to your TRANSUNION score |
| | 669 ACH transaction rejected |



The “USPS Delivery Failure” malware

On December 7th at midnight, the USPS Delivery Failure Notification malware was using an MD5 value of 91c0fc131b4fe42cf2c38e466c9c88fd.



At 5:15 AM it changed to 09015ccf0f0e1f38fa2efb29482da5b5.
At 1:45 PM it changed to 6478d4e2103f59bca6f19a2d93931234.
At 5:00 AM on December 8th that version was still being spammed.
At 5 AM it is not detected by AVG, F-Prot, McAfee, Microsoft, or TrendMicro.
We've been tracking it already for 15 hours at that point.



New Computing Paradigms

- Telecommuting – let's use a personal computer not administered by work to access sensitive data from home
- Mobile Computing – let's put sensitive corporate email on a device with no available security software
- Social Networking – let's click silly videos from near strangers while we sit inside the perimeter
- Cloud Computing – let's send all of our data OUTSIDE the perimeter



“Telecommuting” challenges

- Loss or Theft of devices
- Communication through unprotected channels
- Accessing information on unprotected home devices
- Inappropriate access to information by non-employees residing with telecommuter
- Printed materials without proper disposal options





“Mobile Computing” challenges

Stolen phone – fits in a pocket

If I have your phone, I **AM** you.

Some have called 2011 “The Year of Mobile Malware”

a “Zeus” version that runs on Blackberry
(BBOS_ZITMO)

Android Malware;

- **PJApp** – steals sensitive information
- **GoldenEagle** – records voice calls and forwards to attacker
- **ApkMon** – gains “root” access on phone to read system files and logs
- **Spitmo** – intercepts banking requests for confirmation and “confirms” transactions without notifying user





“Social networking” challenges

How many of your employees are sharing workplace facts “privately” with their Facebook friends?

This week Mark Zuckerberg’s private Facebook data was hacked.

If Mark’s Facebook data isn’t safe, is your employees?





“Cloud Computing” challenges

Threat #1: Abuse and Nefarious Use of Cloud Computing

Threat #2: Insecure Interfaces and APIs

Threat #3: Malicious Insiders

Threat #4: Shared Technology Issues

Threat #5: Data Loss or Leakage

Threat #6: Account or Service Hijacking

Threat #7: Unknown Risk Profile



Top Threats
to
Cloud Computing V1.0

Prepared by the
Cloud Security Alliance
March 2010

<https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>



“Information sharing” challenges

One “cloud-related” threat is the move to ever greater transparency between and within government organizations.

After 9/11 the media, the public, and the Congress took turns kicking the Intelligence community for not sharing information.

Greater information sharing - - homogenous data access available at the fingertips – increases the chances that an insider can access your data and post it to Wiki Leaks or share it with your enemies.





We Want To Help

Gary Warner

Director of Research in Computer Forensics
A Research Partnership between
The University of Alabama at Birmingham's
Department of Computer & Information Sciences
& Department of Justice Sciences

Website:

www.cis.uab.edu/forensics/

Blog:

garwarner.blogspot.com

gar@uab.edu

+1.205.422.2113