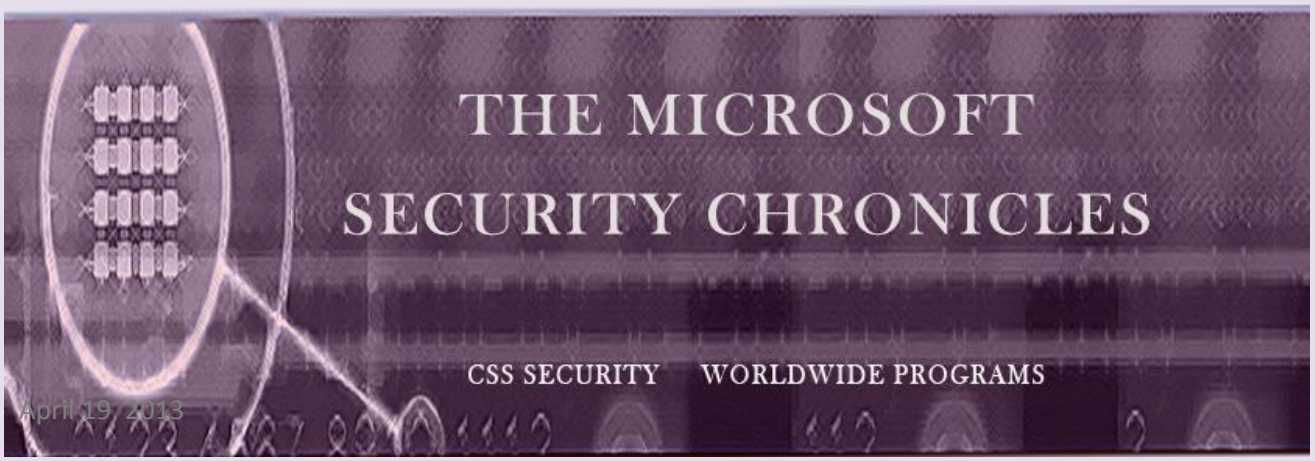

INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

SECURITY CALENDAR

April 2013

15 EuroSys 2013 - Prague

16 SOURCE Boston

18 NotACon – Cleveland, Ohio

DHS Warns of Spear-Phishing Campaign Against Energy Companies

Computerworld

… The alert was prompted by an incident last October in which 11 companies in the energy sector were targeted in a sophisticated spear-phishing campaign apparently aimed at breaching their network security.

Analysis:

Spear-phishing was used in this attack to get access to a company's internal resources. These attacks are becoming more frequent and unfortunately, they are working. The U.S. Federal Bureau of Investigation describes it: "First, criminals need some inside information on their targets to convince them the emails are legitimate. They often obtain it by hacking into an organization's computer network or sometimes by combing through other websites, blogs, and social networking sites. Then, they send emails that look like the real thing to targeted victims, offering all sorts of urgent and legitimate-sounding explanations as to why they need your personal data. Finally, the victims are asked to click on a link inside the email that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc."

One of the things they stress from this story — stop posting too much information on corporate websites! The more information is

19 InfoSec Southwest 2013 – Austin, Texas

23 Black Hat Embedded Security Summit

24 BSides London

25 SyScan Singapore

26 THOTCON - Chicago

27 BSides Chicago

May 2013

02 Hackito Ergo Sum - Paris

09 Microsoft Bulletin Advance Notification

14 Microsoft Security Bulletin Release

15 NoSuchCon - Paris

17 HackMiami

18 BSides Boston

19 BSides Sao Paolo

20 AusCERT - Australia

23 Positive Hack Days - Moscow

23 SOURCE Dublin

28 CONFidence - Krakow

30 RVAsec - Richmond

accessible, the easier it is to attack a company through its employees. The article went on to say that the energy company had posted information about a conference many of the employees had attended (including the employees email addresses, organizational affiliations, and titles). It was then really easy for a spear-phishing attack. Think spear-phishing attacks can't hurt a company — check out this example:

> "For instance, a massive data breach that exposed more than 3.5 million Social Security numbers at the South Carolina Department of Revenue and cost the state millions of dollars in breach notification and remediation costs, began after a *single user [PDF] clicked on an embedded link in a spear-phishing email."*

The U.S. government also issued an alert that too much information on a webpage could cause a company to become the victim of a spear-phishing attack.

Spear-phishing was once thought of as low on the list of something security professionals needed to worry about. It is becoming something that they now need to pay attention. From the article, "It doesn't surprise me at all," said Anup Ghosh founder of security firm Invincea. "Almost every publicized and self-declared Advanced Persistent Threat (APT) attack this year has been through phishing emails." The question now becomes how to educate employees to be aware and to question everything. The emails used to be easy to spot with misspelled words and poor English. Now they are sophisticated, look legitimate, and often from someone they know and trust.

An article in Threatpost states, "A report released Wednesday [March 27, 2013] indicates an organization on average experiences a malware-related event every three minutes, often involving business-related spear-phishing and targeting technology companies." It is very difficult for businesses to stop this kind of attack. The emails are persistent and can be carefully written so that the unsuspecting victim thinks it is from someone they trust.

How does a company or individual guard against this kind of threat? Here are seven ways to guard against these types of attacks:

- Do you deal with this company?

- Don't depend on an email's return address
- Look closely at the email's content
- Know where you are and where you're going
- Search for the message on the Internet
- Use a phishing filter
- Contact the company directly

What should a company do if they have become the victim of a phishing attack? Companies should have contingency plans in place to determine the plan of action such as the following:

- Where should the public send suspicious emails involving your brand?
- What should call center staff do if they hear a report of a phishing attack?
- How and when will your organization notify customers that an attack has occurred?
- Who will take down a phishing site?
- When will the company take action against a phishing site?
- How far will you go to protect customers?
- Are you inadvertently training customers to fall for phishing scams?

The Anti-Phishing Working Group provides a lot of valuable information on their website including advice on phishing, reporting phishing, resources for consumers and businesses, trend reports, and whitepapers. Their latest trend report (published in February of 2013) includes unique phishing sites detected from April – September of 2012, most targeted industry sectors for third quarter of 2012, and phishing reports received to name just a few.

For more information about phishing, check out the Microsoft Safety and Security Center where helpful information such as frequently asked questions, recognizing phishing scams, and preventing ID theft from phishing scams can be found. This additional page provides more in-depth information on phishing scams that target activities, interests, or news events. Also included is a page on email and web scams and how to help protect yourself with a lot of helpful information and links.

Latest Security Intelligence Report Shows 24 Percent of PCs are Unprotected

The Official Microsoft Blog

Today [April 17, 2013], Microsoft released new research as part of its Security Intelligence Report, volume 14, which takes a close look at the importance of running up-to-date antivirus software on your computer. The research showed that, on average, computers without antivirus software are 5.5 times more likely to be infected.

Analysis:

The full version of the Security Intelligence Report (SIRv14) is available now in 10 languages at www.microsoft.com/sir.

Below are some excerpts from the 100+ page document.
Applying and maintaining real-time security software from a reputable vendor and keeping it up-to-date is an important step to reduce exposure to vulnerabilities including malware. The report provides the factual data that mandates users to install real-time antimalware software.

To summarize across the findings of hundreds of pages of new data:

Vulnerabilities
Industry-wide vulnerability disclosures are down almost eight percent primarily because high-severity disclosures dropped 25 percent which muted a 20 percent increase in application vulnerability disclosures. High-severity vulnerabilities made up 30.0 percent of the total compared to 38 percent previously. This was the first time since 2009 application vulnerability disclosures have increased. They had previously seen a steady decline.

Exploits
Exploit activity has increased in many parts of the world. The most prevalent infections were by JavaScript and HTML. The exploit-related family detected most often during the second half of 2012 was Blacole. Blacole is Microsoft's detection name for components of the so-called "Blackhole" exploit kit available for buy or rent from hacker forums or illegitimate outlets. It delivers malicious software through infected websites. Attackers load the kit onto compromised web servers and unprotected visitors risk infection from a drive-by download attack.

The Win32/Pdfjsc exploit more than doubled in the last quarter of 2012 to be the most detected exploit in that period and the second largest in the second half of the year followed by Java exploits. Win32/pdfjsc is an exploit that targets document readers and editors.

Malware

Several locations with historically high malware infection rates saw improvements but the worldwide malware infection rate increased. The top 10 countries were U.S., Brazil, Korea, Russia, Turkey, China, France, Germany, India and the UK.

The U.S. (-15%), UK (-5.8%), Russia (-5.7%), China (-5.2%), and Turkey (-.3%) were countries in the top 10 that experienced a decline in 2012. In the U.S., the fewer detections of the trojan families Win32/Tracur, Win32/Sirefef, and Blacole were the largest contributors to the decline.

India had the largest change and increase at 20.5 percent. Brazil was second overall and had an increase of 13.3 percent primarily because of detections of the adware family Win32/DealPly in the fourth quarter. France (7.7%), Korea (6.5%), and Germany (3.9%) also saw an increase. Detections in Korea rose 52.5 percent between 1Q12 and 4Q12 because of increased detections of the rogue security software family Win32/Onescan. See page 40 of the report for more information about the infection rate in Korea.

The most improved was Pakistan according to the report after normalization and the countries with the least infections were Denmark, Finland, and Japan.

Operating system infection rates for Windows server and client were also included in the report. Windows 8 has the lowest malware infection rate of any Windows-based operating system observed to date. The report said the real-time antimalware protection Windows Defender may be a contributing factor to the low infection rate.

Threat Categories

The following is the list of leading types of threats Microsoft has grouped based on similarities in function and purpose.

- Trojans
- Potentially unwanted software
- Adware
- Worms

- Exploits
- Trojan Downloaders & Droppers
- Viruses
- Password Stealers and Monitoring Tools
- Backdoors
- Spyware

Figure 34. Threat category prevalence worldwide and in the 10 locations with the most detections in 4Q12

Category	Worldwide	US	Brazil	Russia	Korea	France	Turkey	China	Germany	India	UK
Adware	21.2%	20.8%	40.8%	9.3%	32.6%	41.1%	11.1%	3.8%	18.8%	14.6%	23.9%
Misc. Potentially Unwanted Software	33.6%	20.0%	38.0%	50.0%	9.7%	34.1%	38.7%	49.0%	29.2%	38.6%	30.5%
Misc. Trojans	34.0%	43.9%	17.1%	37.1%	75.6%	20.0%	34.7%	32.1%	27.2%	34.7%	29.8%
Worms	17.6%	5.6%	15.7%	17.5%	3.1%	9.4%	34.7%	12.5%	9.2%	39.9%	6.8%
Trojan Downloaders & Droppers	10.4%	9.6%	16.7%	12.6%	9.1%	9.2%	10.0%	14.5%	7.1%	5.5%	9.5%
Exploits	14.5%	23.0%	4.8%	14.2%	4.2%	11.7%	9.0%	6.4%	27.0%	14.6%	23.8%
Viruses	7.7%	2.0%	6.6%	5.5%	1.4%	1.8%	16.5%	15.2%	2.8%	23.8%	3.1%
Password Stealers & Monitoring Tools	5.8%	5.2%	10.5%	5.0%	2.7%	3.5%	4.8%	3.5%	8.8%	7.6%	6.2%
Backdoors	3.7%	2.7%	2.5%	2.9%	1.4%	2.4%	5.0%	6.3%	2.5%	6.4%	3.0%
Spyware	0.2%	0.3%	0.0%	0.2%	0.0%	0.1%	0.0%	1.2%	0.2%	0.1%	0.1%

Totals for each location may exceed 100% because some computers reported threats from more than one category.

Miscellaneous trojans topped the list of malware threats coinciding with previous SIR releases.

In Korea, families in the miscellaneous trojans category were detected on 75.6 percent of all computers that reported detections mostly because of Win32/Onescan.

In Brazil and France, adware was detected on more than 40 percent of computers reporting detections in each location. The most commonly detected family in France in 3Q12 was Win32/EoRezo, an adware program that delivers French-language advertisements. The miscellaneous potentially unwanted software category was also unusually prevalent in Brazil, with Win32/Keygen the most commonly detected threat in the category in 4Q12.

In the U.S., UK, and Germany exploits were unusually common due to Blacole and Win32/Pdfjsc being among the most common exploit families detected.

In Russia, the miscellaneous potentially unwanted software category was especially prevalent, led by Keygen and Win32/Pameseg. Pameseg is a family of installers that require the user to send a text message to a premium number to successfully install certain programs, some of which are otherwise available for free. Currently, most variants target Russian speakers.

In China, Keygen was detected on almost half of the computers reporting detections, making the miscellaneous potentially unwanted software category especially prevalent there. Spyware was also unusually prevalent in China, led by Win32/CnsMin. Although spyware was the least prevalent category in China, it was more than six times as prevalent there as in the world overall.

In Turkey and India, worms were unusually prevalent led by INF/Autorun. See "Appendix C: Worldwide infection rates" on page 89 for more information about malware around the world.

The SIRv14 includes other topics:

- Rogue security software
- Home and enterprise threats
- Email threats — spam volumes have gone up slightly. More information is available on spam messages blocked and spam message types. Guidance on malware and email threats.
- Malicious websites — phishing sites and malware hosting sites including global distribution
- Bing on drive-by download sites

Last word: Installing and using real-time antimalware software help individuals and organizations reduce malware infection by more than 80 percent. See www.microsoft.com/windows/antivirus-partners for a list of vendors that provide consumer security software solutions for Windows.