

Zeus Attacks Vermont

It appears that the Zeus Trojan is plaguing financial institutions in this region. The problem is that Zeus only infects the customer's machine and then steals personal data during an online transaction. The institution's networks are not compromised and the whole transaction appears perfectly normal to them. Zeus can insert fields and windows that only the customer sees, do this without breaking the SSL connection with the host, and the inserts exactly match the normal online screens. The customer innocently fills in the added fields that call for personal data, such as their account number or PIN, which Zeus then sends directly to the attacker. The remaining fields are sent as normal to the company. Because each instance of Zeus is customized and there are many quickly changing variants, anti-virus software has not yet kept pace. The detection rate may be as low as 30%. From the host side, the company does not know there is a problem until later when they may spot an account being drained. So far, the only sure fix is to wipe the customer's hard disk.

Just what is Zeus? The bots are obviously searching millions of PCs, but how does Zeus connect a customer with a financial institution? Are they indicators such as application code or a cookie used by a particular institution? How does Zeus get hold of the transaction screens so their inserted fields or windows exactly match the originals? How is this happening despite the encryption? Is there possibility of social engineering component to trick a customer to click on something that then downloads the Trojan? These are questions not easily answered. Still, there must be discernable patterns that an institution can detect even though signature detection is not feasible.

It is not likely that anti-virus software can help much. Moreover, do not expect much help either from law enforcement for they lack the resources. As they shut down a few bots, countless more pop up. Nor are the individual institutions, their industry associations or consultants able to help much. They too lack the resources or enough information to develop countermeasures. InfraGard, however, can provide valuable assistance. We are uniquely qualified to share and exchange information anonymously and in confidence and to collaborate effectively with both the private and public sectors. We can at least help everyone know what is happening and what to look out for, so that someone can develop effective solutions.

Here is more information taken verbatim from the DHS Daily Open Source Information Report:

February 9, DarkReading – (International) New banking Trojan discovered targeting businesses' financial accounts. The infamous Zbot botnet that spreads the pervasive Zeus Trojan has been seen distributing a brand-new banking Trojan — one that researchers say could serve as a lower-cost alternative to the popular Zeus and Clampi malware for cybercriminals. The new Bugat Trojan, which was discovered by researchers at SecureWorks, appears to be aimed at mostly business customers of large and midsize banks. It is built for attacks that hack automated clearinghouse (ACH) and wire transfer transactions for check and payment processing — attacks in which U.S.-based SMBs and state and local governments are losing an average of \$100,000 to \$200,000 per day, according to data from Neustar. To date, Zeus and Clampi Trojans have mostly been used for stealing financial credentials. But a security researcher with SecureWorks' Counter Threat Unit (CTU) says Bugat has some of the same features as other banking Trojans, but with a few twists: It uses an SSL-encrypted command and control (C&C) infrastructure via HTTP-S, and also goes after FTP and POP credentials via those encrypted sessions. The researcher says SecureWorks has witnessed around 1,200 to 3,000 Bogat attack attempts during the past week against its clients. "We saw in the wild that it was being distributed from a specific

Zeus botnet,” he says. “Oddly enough, its purpose is the same as Zeus ... but it’s something not as recognizable as Zeus or that’s cheaper [to purchase] in the long term.” Bugat’s main targets so far are business financial accounts. Source: http://www.darkreading.com/vulnerability_management/security/client/showArticle.jhtml?articleID=222700615&subSection=End+user/client+security

February 9, Computerworld – (International) New Russian botnet tries to kill rival. An upstart Trojan horse program has decided to take on its much-larger rival by stealing data and then removing the malicious program from infected computers. Security researchers say that the relatively unknown added this functionality just a few days ago in a bid to displace its larger rival, known as Zeus. The feature, called “Kill Zeus,” apparently removes the Zeus software from the victim’s PC, giving Spy Eye exclusive access to usernames and passwords. Zeus and Spy Eye are both Trojan-making toolkits, designed to give criminals an easy way to set up their own “botnet” networks of password-stealing programs. These programs emerged as a major problem in 2009, with the U.S. Federal Bureau of Investigation estimating last October that they have caused \$100 million in losses. Trojans such as Zeus and Spy Eye steal online banking credentials. This information is then used to empty bank accounts by transferring funds to so-called money mules — U.S. residents with bank accounts — who then move the cash out of the country. Sensing an opportunity, a number of similar Trojans have emerged recently, including Filon, Clod and [Bugat], which was discovered just last month. Source: <http://www.computerworld.com/-s/article/9154618/New-Russian-botnet-tries-to-kill-rival>

There are indeed serious and growing problems here and critical shortcomings in everyone’s ability to protect and defend. Law enforcement and the financial institutions are already stretched thin and continue to lose ground as more and more attack vectors emerge. InfraGard is in a unique position to assist and support. We need to expand our outreach and form sectors within critical industries (such as a banking sector) that can better share information, work with associations, developers and consultants, and better report details to law enforcement.

Ten Top Botnets

For a list of the top-10 botnet outbreaks in 2009, visit <http://blog.damballa.com/?p=569>. And for more discussion including some long-dead botnets that keep returning, visit <http://www.darkreading.com/insidertreat/security/client/showArticle.jhtml?articleID=222900762&subSection=End+user/client+security>. These surveys are, of course, more or less a best guess covering only the attacks discovered and reported. The exploits shown may be far too few, because many organizations attacked are keeping silent for fear of reputational damage. However, these data give some idea of the huge economic costs of botnet outbreaks.

Still Another Risk?

The following is also from the DHS Daily Report: February 11, WHDH 7 Boston – (National) Report: Terrorists planning breast implant bombs. Reports say terrorists could begin hiding explosives in breast implants. British spy satellites have reportedly intercepted terrorist communications from Pakistan and Yemen, talking about women suicide bombers getting explosives put inside breast implants. The former Houston FBI director said he believes U.S. Homeland Security is taking this threat very seriously. “Sometimes as ridiculous as it may sound, it can probably be pulled off...Terrorists and terrorist attack are a reality,” he said. The British Intel service reports several plastic surgeons who were trained in many of London’s hospitals have returned to their countries to perform the surgeries. “I’m sure we are gathering all the information, intelligence that the government can,” he said. “They are also securing all

the ports, airports and main attractions as much as possible. The government takes these types of threats seriously and not relaxed.” A Houston plastic surgeon said that the industry’s technology makes the bombs possible and easy. The Transportation Security Administration says its scanners do detect explosive materials and residue. However, it is unknown how well full-body scanners would detect explosives inside implants. Source: <http://www1.whdh.com/news/articles/local/BO135406/>

And if terrorists can indeed implant boob bombs, they can also implant explosives to mimic pregnancy or obesity in men, women, children, or perhaps live animals as well. There are already many reports of women, couples, children and even babies concealing bombs – also bombs placed within dead bodies or animals is commonplace -- and at least one report of a bomb implanted within an individual but no details. While some of the possibilities might only be tabloid fodder, there are questions and there may well be ways to detect such threats. First, how are they going to detonate? Wires hanging out or batteries inside will show up on x-rays and probably metal detectors as well. There are already many shortcomings in searching persons for hidden explosives, especially when only a patdown is possible. Increasingly, security guards and police need to be experienced in dealing with a potential suicide bomber and areas of the body where explosives may be concealed, internally or externally.

Finally

During testimony at an open hearing of the Senate Select Committee on Intelligence on February 2, the Director of National Intelligence, the CIA Chief, and the FBI Director were each asked about the likelihood of another terrorist attack on the U.S. homeland in the next three to six months. Each replied independently that such an attempt is certain. The media and the bloggers exploded with accusations of sensationalism and fear mongering. However, let’s look behind the headlines and consider what they might believe will happen sooner or later.

The hearing was televised on C-SPAN¹. There is also a short FBI report on the secure InfraGard Web site for members to read; the title is *Terrorists Maintain Intent to Attack the United States*. Members cannot disclose the contents and the file is locked to prohibit saving, printing or copying. However, if one pokes around a bit on the Web, it is clear that officials are concerned, especially about attacks planned by someone we could never hope to know. Though not mentioned, many attacks are probably coming at us – a few very large (which was the question asked), but also many small, widespread attacks on non-prime targets to distract and disrupt us.

No one doubts that many groups are committed and determined to destroy America. There are already thousands of these people worldwide and the number is fast growing. Most are fully radicalized, well trained, financed, and equipped and their activities well concealed. While some are plotting traditional attacks, most are devising new ways to kill and destroy that we have generally not thought about yet. While we tend to prepare for history to repeat itself, the terrorists are developing new approaches, better technology, and using extensive experience gained in Iraq and elsewhere. The likelihood is that we will soon see many new and different threats as well as new adaptations of the old ones. Whether you agree that this is “certain” is up to you.

Al Qaeda and its major divisions are surely plotting hard to inflict a major disaster on the U.S. homeland. Also, there are perhaps thousands of little-known small cells and lone-wolf individuals who are

¹ The Director of National Intelligence, Dennis Blair, testified again to explain more on February 12 in an open hearing before this committee. There is a video of the hearing streamed on www.c-span.org.

well trained and radicalized and waiting for an opportune moment to attack. There are maybe thousands of foreign and domestic terrorists already in this country, and many more working here, immigrating, visiting or sneaking in. They are not likely to try mega-attacks. Instead, their mission is to carry out many, small, widespread attacks, probably on non-prime soft targets. Their goal is to create chaos, draw us away from prime targets and divert attention from major attacks that al Qaeda is planning. Officials are concerned that we have too few resources and very little intelligence and that we are not prepared to cope with attacks that do succeed.

Let's look harder at the individuals and smaller groups, what threats they may pose and their chances of success. The favorite terrorist weapon is the suicide bomb and there are many variants that don't necessarily kill by exploding. Increasingly, the terrorists here will know how to use bombs effectively. And since most of these people are still unknown, they can move about the country freely and purchase the weapons and materials needed without attracting much attention.

However, there are discernable patterns to their activities and many unusual or suspicious events that can be observed as they plan and set up an attack. If the public can recognize and report these events to the FBI, law enforcement can be alerted to previously unknown trouble spots. With the public's help, officials will be better able to connect the dots, collect evidence, capture those involved, and prevent trouble. Without our help, the likelihood of successful attacks – many attacks – is almost certain. InfraGard can play a vital role.

Yes, but why should we interfere? We are not law enforcement; we are not trained; it is not our job; and besides, it is their responsibility to protect us. Accordingly, many persist in not telling law enforcement what they need to know to protect us. This is dangerous thinking. The fact is that we at the local level are both the first and the last lines of defense. It is therefore our responsibility to protect ourselves and others as well. We must know what to look for and be vigilant.

Very possibly, there may soon be a wave of small terrorist attacks throughout the United States, most by suicide bombers. Probably attacks on unlikely targets, public and private. Suicide car and truck bombs are effective ways to destroy buildings, religious places, bridges, infrastructure, utilities, dams and large gatherings. There may also be suicide missions using boats or small aircraft. Likely, they will also use persons as suicide bombers to get closer to their targets. And there may be non-explosive WMD devices used. All are potentially dangerous and disruptive and some may be decoy attacks. The martyrs may be one or more drivers, bombers, or others sworn to fight to the death. There may also be a second person or vehicle to trigger the bomb(s) or to videotape the event to assure publicity and to claim credit. Once such an attack is set in motion, it is hard to stop.

However, there are many discernable patterns in planning and setting up most of these attacks. There is usually a terrorist cell and each person will have roles to play that are in themselves unusual, some obviously suspicious when they believe that others won't bother to report them. Their planning involves much surveillance and intelligence gathering, finding the best route and point of attack, trial runs to determine the timing, staging of supplies and perhaps guns as well, and maybe planting multiple bombs. There are also final preparations for martyrdom by the participants themselves. Each element is usually a phase of the attack plan, and each has unusual and distinctive patterns that can be recognized and reported.

The Department Homeland Security provides useful information on such patterns, ways of doing surveillance, the appearance of bombs, how to protect yourself, and how to handle suspected bombs or bombers. Some InfraGard members have access to this material and we can share it with others who

should be aware. Persons within the business sectors with a need to know can also access this material, if they even know it exists. Most of the DHS material is very well done and far better than is available elsewhere.

We in InfraGard can play a valuable role in sharing and exchanging this information widely among the private and public sectors, doing this anonymously and in confidence, and in making sure it is reported to the FBI and other law enforcement. We can be a valuable catalyst to achieve much better security. However, as IVMA we also need to expand our outreach and build ties to a wide range of organizations and agencies. We need to form sectors within industry groups and associations. And we need to expand our membership to include more experts and others who need to know more about infrastructure security.

Once people and property can be better protected, what about continuity planning? Will there be continuity of management if trouble happens? How about the ability to maintain critical operations when trouble comes? Is there sufficient backup and redundancy to continue operations when the Internet and telephones are unreliable? What if your people must evacuate, or building power is shut down, or there is severe smoke or flooding from a fire in the region, or when no one can access the site? These and more questions all require good answers or management will be in a lot of difficulty.

InfraGard can provide many valuable resources and we are uniquely qualified and positioned to do so. We can: 1) Become a reliable resource to report unusual events to law enforcement and provide local knowledge that police simply cannot obtain until after a crime is committed. 2) Share and exchange information in confidence among and between both the private and public sectors. 3) Validate preparedness: Review and check risk assessments, vulnerability analyses, response plans and procedures, and help with implementation including training and awareness, exercises and drills. Our members are subject experts in all of these areas and can assist as independent facilitators with no commercial affiliation. (Members who are interested can also be paid at least an honorarium and expenses.)

If more attacks are considered a certainty, is the public prepared and vigilant, and are we as IVMA ready to provide what can be valuable assistance to both the public and the private sectors?

As always, comments, suggestions and contributions are welcome.

Frank Platt, IVMA VP and Editor

[This space is available for members to list announcements, their products or services, post links to interesting sites, or contribute material of public interest. Submissions may be edited for brevity and to reduce commercial content.]

Franklin N. Platt
Office Planning Services

55 Paris Road
Stark, NH 03582

Tel: (603) 449-2211
Email: Fnplatt@aol.com

Profit from Good SecuritySM

Security Preparedness & Compliance since 1967

• Risk Management • Analytics • Due Diligence • Second Opinion • Validation • Training
