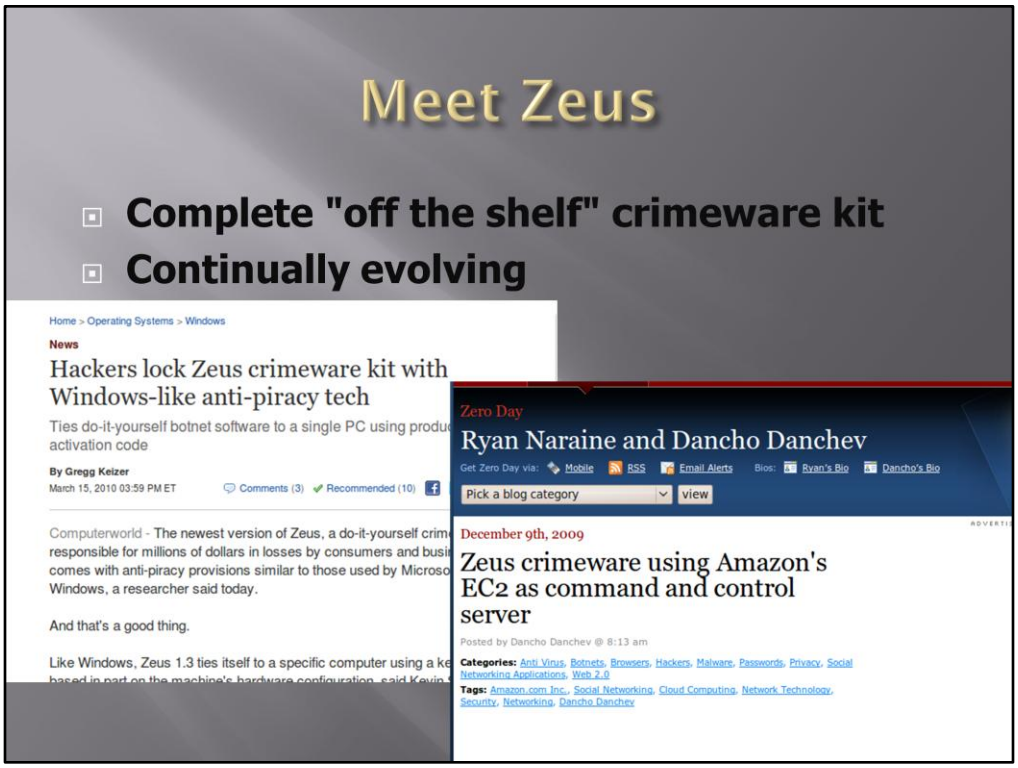


http://www.computerworld.com/s/article/9170978/Hackers_lock_Zeus_crimeware_kit_with_Windows_like_anti_piracy_tech
http://blogs.zdnet.com/security/?p=5110

Zeus is a commercial off-the-shelf software package for committing computer crime. Primarily targeted at banking fraud, the Zeus crimeware includes functionality for keystroke logging and screen captures, "man in the browser" exploits to intercept and use even one-time password credentials, and remote control of infected PCs, among many other pieces of functionality. For a few thousand dollars on an underground forum, anybody can purchase a copy of Zeus and create a business model for themselves that can net millions of dollars in illegal gains.

Like any legitimate software package, Zeus requires purchasing of a product activation key. Customer support is available, with different support tiers including direct support from the author of Zeus for premium customers. And like modern software companies, Zeus has (at least in an ad hoc fashion) developed its own "cloud strategy" as Zeus command and control servers move into infrastructure providers like Amazon EC2.

And yet Zeus itself is just one piece of a larger criminal ecosystem that has developed over the last decade, which include a wide variety of services necessary for perpetrating these crimes:

• Exploit kits such as "Black Hole" which provide an infection vector for the Zeus malware
• "Bullet-proof" hosting services that provide guaranteed uptime for command and control servers and SLAs that rival many commercial infrastructure as a service providers
• Money mules receive small transactions from victim companies and wire them to intermediate accounts. "Mule herders" provide mules based on geographic needs, bank type, account limit, and other factors
• Individuals that "cash out" funds from the intermediate accounts and transport the funds across borders

And if all of this is too much work for somebody looking to get started at this kind of criminal enterprise, a "software as a service" model has developed where you can simply rent somebody else's Zeus botnet. Or you can simply be one of those who lives on the side-effects of these crimes– trading in stolen credit cards or conducting various identity theft scams using the credentials stolen by Zeus.

So if this new millennium we find ourselves in has brought anything, it's the growth of computer crime as a business…

http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring

And a very good business it is too, at least for some groups. In October 2010, the FBI issued a press release regarding an investigation code-named "Trident Breach". They were investigating an international group of organized cyber-thieves who were using the Automated Clearinghouse (ACH– hence "Trident BreACH") system to steal millions of dollars from US businesses. The press release quotes total thefts at US$70mil, with over US$200mil in attempted thefts.

This was a large multi-year investigation for the FBI. But even if that US$70mil was stolen over multiple years, who wouldn't be satisfied with being in charge of a business whose gross income was tens of millions of US dollars per year? So it's small wonder that at any given time, there are multiple organized criminal gangs using software like Zeus to pursue their money-making schemes.

But of course, their success is based on stealing wealth from other legitimate businesses. So unlike a normal enterprise whose success creates new economic opportunities, these criminal enterprises actually end up having an extremely negative economic impact. Many small business have been driven *out of business* due to losses incurred by Zeus fraud. And of course, this means lost jobs, and further downstream economic impacts.

Ultimately, you can view even nation-state cyber attacks from an economic rather than military/strategic perspective. In fact, many nation state attacks are targeted directly at capturing valuable intellectual property to further a nation's economic goals. To the extent that these attacks target military or strategic targets (uranium enrichment plants or power grids) it's because the nation that's masterminding the attacks has made the economic decision that cyber intrusion is a more cost-effective way to pursue their strategies than kinetic warfare.

And yet as successful as these attacks have been, and despite unprecedented financial losses, not all of the news is bad. The Trident Breach investigation showed what can be accomplished by a dedicated team of international law enforcement agencies. Trident Breach even involved law enforcement from Eastern European nations, which have historically been unwilling to cooperate with Western law enforcement. While the masterminds behind the ACH fraud scam were not apprehended, several other participants were captured, tried, and incarcerated, essentially crippling the criminal nexus and undoing years of careful planning and development.

http://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/

In fact, the pressure from the FBI investigation even caused the author of Zeus to sit up and take notice. Shortly after the Trident Breach arrests, the author of Zeus– who generally goes by the nickname "Monstr" on various underground forums– announced that he was getting out of the business of updating and supporting Zeus. More surprising, Monstr announced that he was giving over the Zeus technology and support contracts to "Harderman", the author of the SpyEye trojan, and Monstr's upstart competitor.

Monstr's announcement seemed like an enormous bombshell to those who'd been following the Zeus v. SpyEye fracas on the underground forums. And yet Monstr had "retired" before when the heat got turned up to high on his software and the gangs who were using it. Zeus has always come back stronger than ever, Monstr apparently having taken his "time off" to develop new features and new ways for the software to escape detection.

http://news.softpedia.com/news/Man-in-the-Mobile-Component-Spotted-in-SpyEye-193344.shtml
http://www.computerworld.com/s/article/9227387/Banking_malware_spies_on_victims_by_hijacking_webcams_microphones_researchers_say?taxonomyId=83

Harderman, in turn, announced plans to merge the best features of Zeus and SpyEye into a single super-trojan. One of the first signs of the merger was SpyEye inheriting Zeus's mobile device trojan technology. After all, every modern software provider has to have a mobile strategy, right?

Particularly in Europe, transaction verification via one-time codes sent to mobile devices has become common. Monstr developed a mobile trojan for Symbian phones that intercepted these Mobile Transaction Authorization Numbers (mTANs) and transmitted them to the Zeus botmaster, and Harderman simply adapted the idea for the new SpyEye. This shows the ongoing "arms race" and flexibility of the "black hats" in these scenarios. As we move to mobile platforms for convenience and flexibility, the bad guys follow because that's now "where the money is".

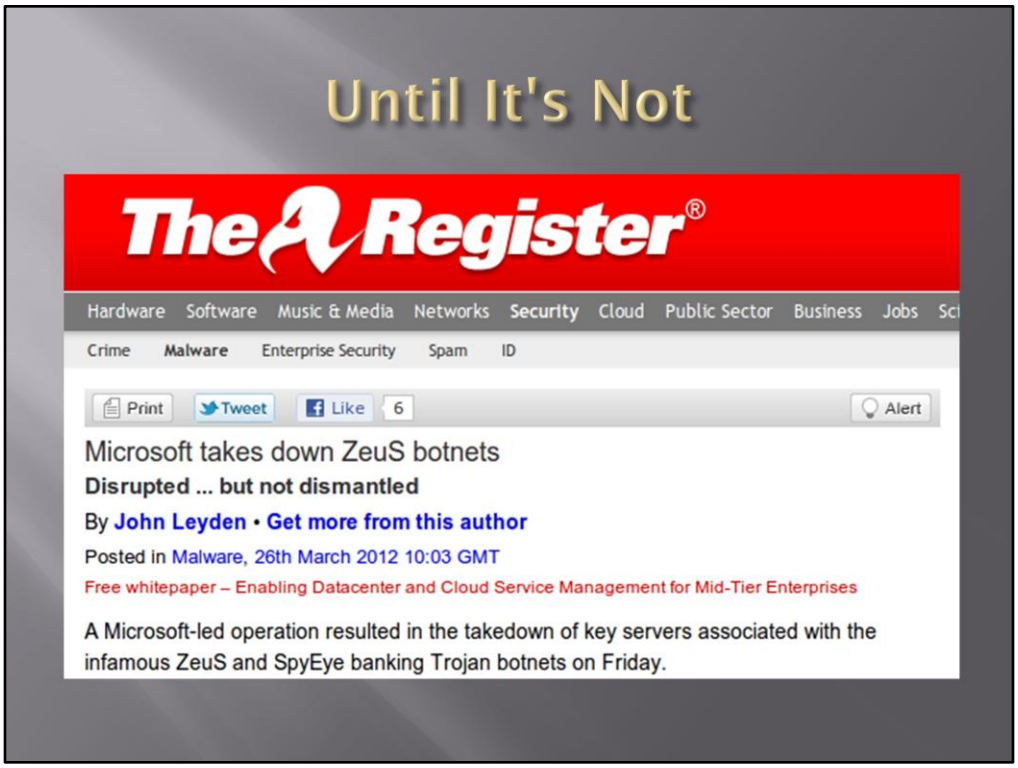
Another common out-of-band transaction mechanism is for banks to call customers and have them verify "high risk" transactions using "secret questions" or other private financial details. Recently, plug-ins for SpyEye have been observed in the wild that can silently activate the user's web-cam and microphone as a means of eavesdropping on these conversations. Once this information has been overheard, the bot-owner can successfully pose as the account-holder and completely compromise the account.

In addition, to the extent that the SpyEye trojan uses fake pop-ups and other messages within the user's browser to trick them into revealing information to help compromise their account, this new spying functionality in SpyEye helps the bot masters to assess in real-time how effective their social engineering tactics are. Just like any legitimate business would test the effectiveness of a marketing campaign in influencing consumer opinion, the SpyEye bot masters now have access to a rich platform for adapting their campaigns for maximum effectiveness.

With the merger of Zeus and SpyEye, Harderman effectively had a monopoly on the COTS banking trojan market segment. It appears that this may have been something of a "success disaster" for Harderman. His customers found him progressively more difficult to reach in the normal support channels, and recently Harderman seems to have largely disappeared from the usual underground forums he was known to inhabit.

In the meantime, a fairly robust community has grown up around SpyEye, using the software's plug-in architecture as a framework to support new community-developed modules. This has the flavor of similar community supported projects in the legitimate software world that have sprung up after the vendor has ceased to support a popular tool. The fact that there is a substantial enough community of SpyEye users to continue development of the tool in an ad hoc fashion tells you something about the size of the community using it.

It's possible that Harderman's behavior is a ploy similar to Monstr: going on hiatus for a while to avoid potential criminal investigation. Perhaps Harderman even had warning that something was going on, because the next chapter was about to be written.

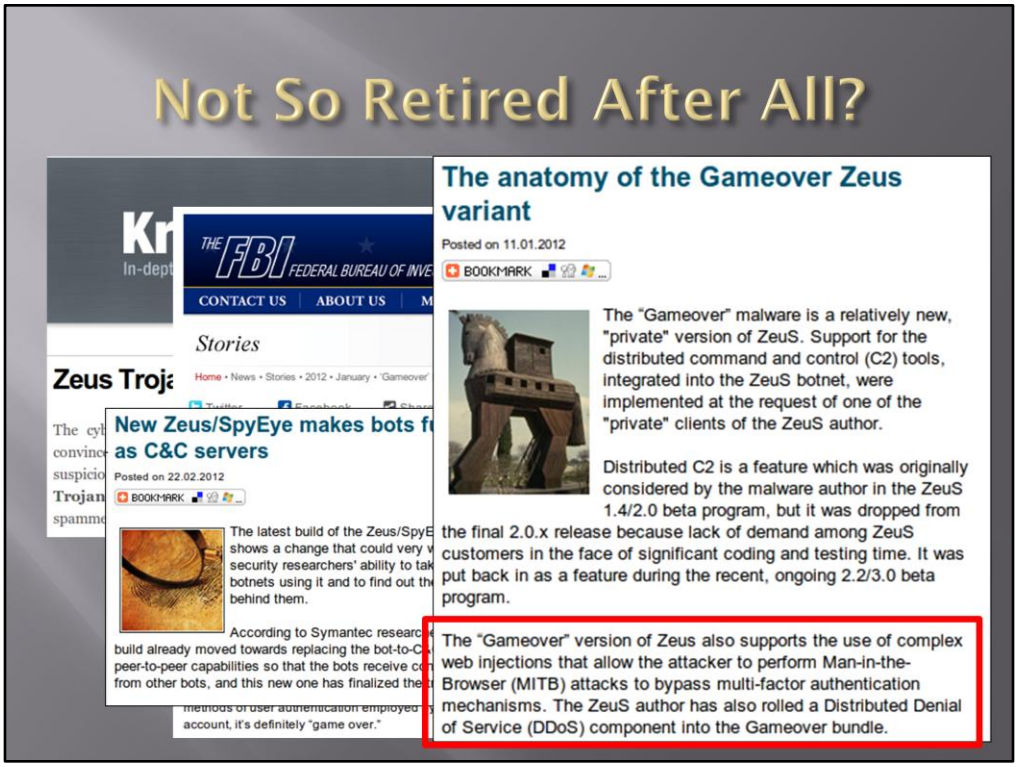


http://www.theregister.co.uk/2012/03/26/zeus_botnet_takedown/
http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232900239/controversy-erupts-over-microsoft-s-recent-takedown-of-a-zeus-botnet.html
http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/

In March of 2012, Microsoft brought civil suit against 39 "John Doe" defendants regarding their Zeus/SpyEye related activities. On the basis of the suit, Microsoft received authorization to raid two hosting providers where Zeus/SpyEye command and control infrastructures were believed to be housed, taking the C2 serves offline and disrupting major botnets.

While the operation was a success from Microsoft's perspective, temporarily disrupting major Zeus/SpyEye botnets, there was enormous outcry from the security research community and law enforcement agencies who were aware of the location of the C2 servers seized by Microsoft and who had been leaving them running to gather additional intel to aid in their investigations. Microsoft's unilateral action damaged these ongoing investigations and caused the criminals to relocate their C2 servers, which must now be tracked down again. There was also damage to already shaky trust relationships among law enforcement, public-, and private-sector organizations who will now be more reluctant to put information out into the community that might lead to similar actions.

Microsoft in an interview after the takedown said that operational security was the primary reason they didn't warn the rest of the community of the impending takedown. And indeed it's hard to imagine how Microsoft could have identified all of the potential stakeholders and provided notification in such a way that it wouldn't have leaked back to the botnet operators. This will continue to be an ongoing issue as more private organizations look to take on computer criminals who are damaging their business interests.



http://krebsonsecurity.com/2012/02/zeus-trojan-author-ran-with-spam-kingpins/
http://www.fbi.gov/news/stories/2012/january/malware_010612
http://www.net-security.org/malware_news.php?id=2009
http://www.net-security.org/malware_news.php?id=1959

When we last left Zeus author "Monstr", he had announced his plans to get out of the malware business. But later research also indicated that Monstr was not only the author of Zeus, but also heavily involved in spamming activities. Indeed Zeus-infected machines always had the capability of being used to send spam, so this was one potential aspect of the Zeus business model.

Starting in early 2012, we began to see public discussions of a new Zeus variant that was not connected with Harderman's Zeus/SpyEye merger product. This new malware, dubbed "Zeus v2" or more popularly "Game Over" appears to have been a bespoke development effort for one or more of the more successful organized Zeus gangs. It appears that Monstr had not really "retired", he'd merely moved into a private consulting arrangement for those that could afford to hire him directly. Certainly any legitimate business that was making tens of millions of dollars per year could afford to hire an army of programmers (or a small number of extremely good ones) to support their core business. From Monstr's perspective, the situation must have seemed like a low-risk, high-reward opportunity.

The new Zeus variant adds a DDoS capability, which is potentially fueling the rise in "extortion" cybercrime– "pay us X or we'll take down your e-commerce infrastructure". In June 2012, arrests were made in relation to just such an extortion scheme targeting the Hong Kong Gold and Silver exchanges.

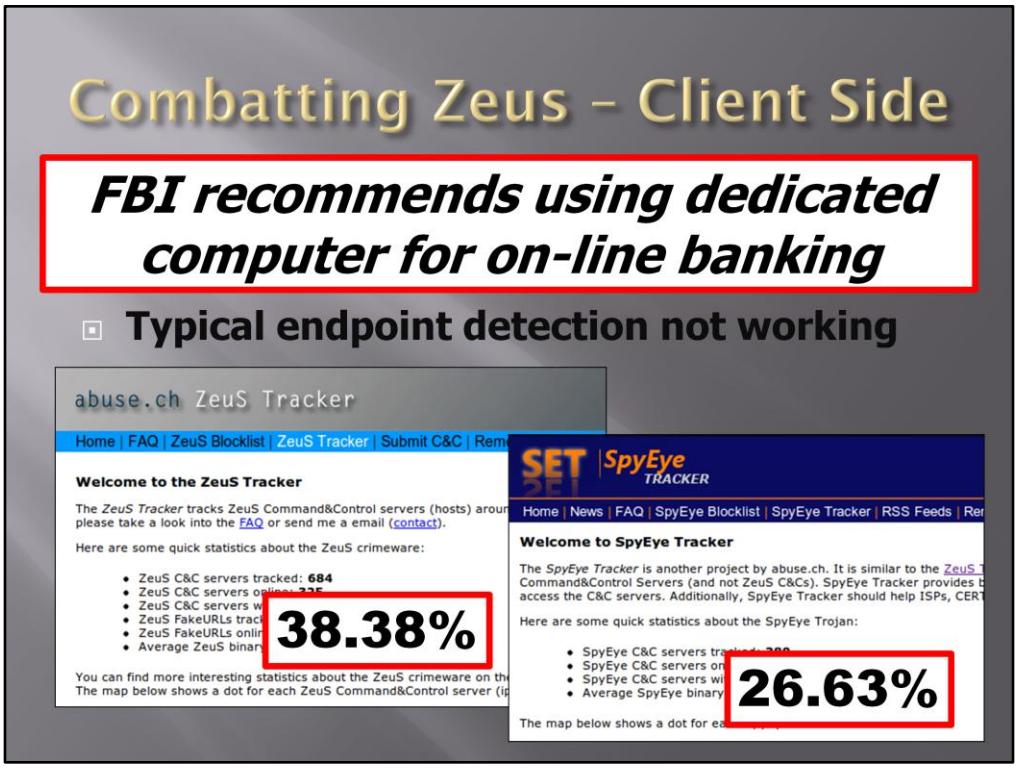
More troubling is that Game Over supports a peer-to-peer command and control infrastructure. By allowing any compromised machine to function as a command and control server for any other machine in the botnet, the botnet becomes more resistant to a Microsoft-style takedown. It also interferes with common enterprise tactics for disabling infected systems, such as black-holing known C2 servers.

http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1373452,00.html

And the cyber crime business is booming. Organized criminal gangs using the Zeus v2 malware continue to steal tens of millions of dollars from the US and other Western European nations. The only thing that's stopping Monstr from developing even more Zeus technology is the fact that the current version is working so well, there's no need to make the effort.

US SMEs are failing when their funds are stolen because US business accounts are not federally insured against these kinds of losses the way individual depositor accounts are. And when a small business fails, there are ripple effects as jobs are lost. Depending on the figures you believe, as much as 80% of the US workforce is employed by companies with less than 100 employees. So these small business losses cut directly at the economic engine of the US.

And there's also pushback on the banking industry. If the banks make good their customers' losses, then it hits the bank's bottom line or gets passed onto their customers as higher fees. If the banks refuse to make the losses good, then the victim companies or their insurers bring suit and nobody wins but the lawyers.



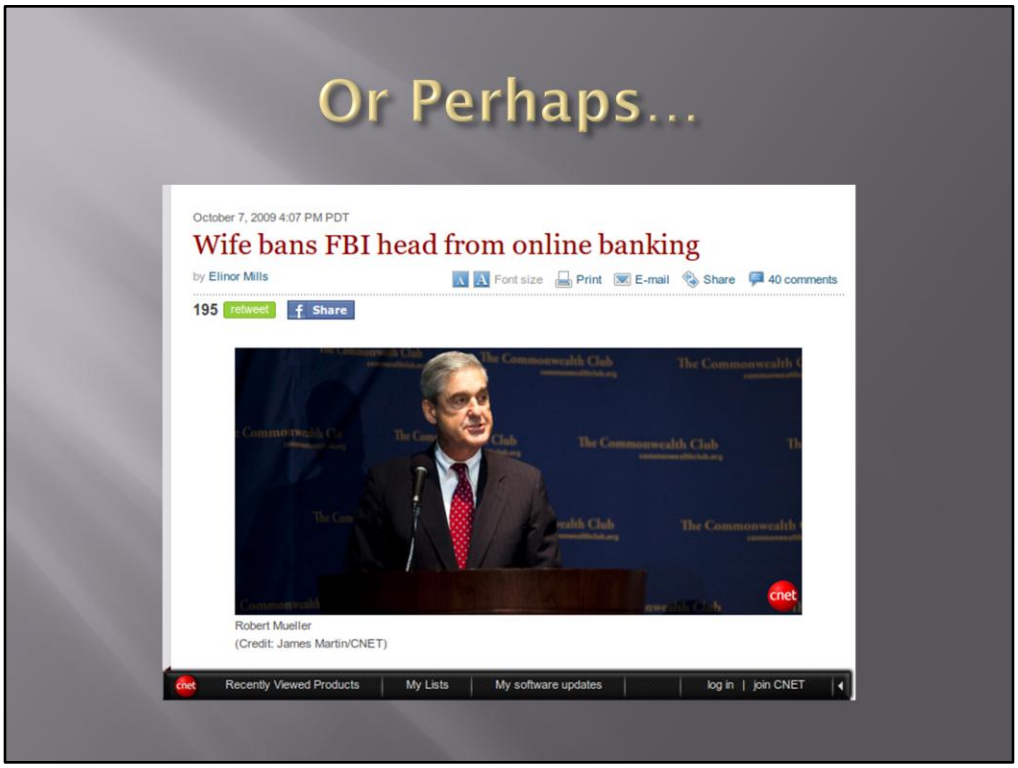
https://zeustracker.abuse.ch/
https://spyeyetracker.abuse.ch/
http://www.usatoday.com/tech/news/computersecurity/2009-12-30-cybercrime-small-business-online-banking_N.htm

So what's a small business to do? At this point, the only answer seems to be, "Prepare to be a victim." Standard end-point protection schemes that SMEs rely on for most of their security are completely ineffective at blocking or even detecting the presence of the Zeus and SpyEye malware. Exploit kits like Black Hole include new exploits at a faster rate than most SMEs can keep up with. And the "attack surface" of a normal PC is vast.

The FBI recommendation is to use a dedicated PC for all on-line banking activity, but that is really beyond the means of many SMEs. And the reality is that eventually that PC is going to be used for something other than on-line banking and will become infected.

Booting from alternate media, such as a Linux CD, and doing financial transactions might work for a home-user or a small business. But when businesses drive their finances out of a custom financial software package (Quickbooks, JD Edwards, etc), such an approach won't work.

In the meantime, review your business account balances regularly to detect fraud. If your bank supports out-of-band transaction confirmations, use them. If possible, require that all transactions be created by one individual but approved by a second, just to make the attackers' job harder.

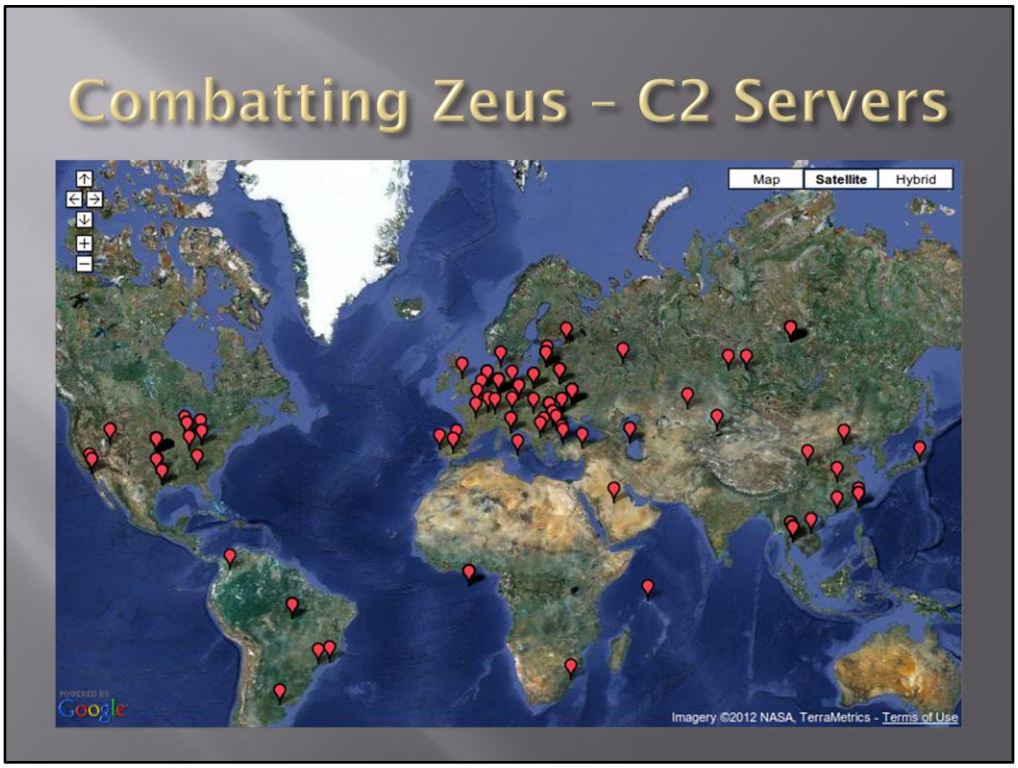


http://news.cnet.com/8301-27080_3-10370164-245.html

During remarks made at a Commonwealth Club event, FBI Director Robert Mueller told an anecdote of nearly falling for a bank phishing scheme. When he tried to use the event as a "teaching moment" with his wife, she forbade him from further online banking activities.

While this was a juicy press moment, the underlying implication is that the continuing success of on-line banking crimes will ultimately have an impact on consumer confidence in online banking. Banks have a vested interest in their customers continuing to use online banking, since it represents an enormous potential for cost savings over traditional "bricks and mortar" bank branches. If consumers start to abandon online banking as "unsafe", this will also have negative economic impact on banks, and their customers who will have to at least partially defray the cost to the banks in the form of higher fees.

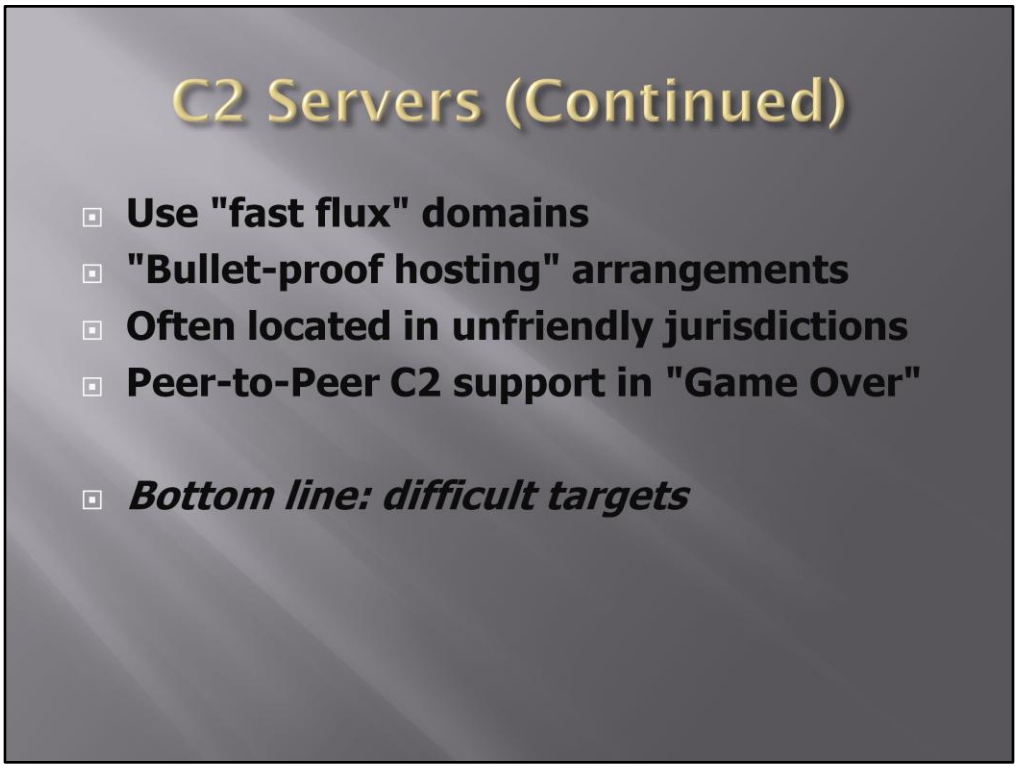
It's a wonder that more banks aren't taking actions similar to Microsoft, in an attempt to disrupt some of the more successful organized gangs.



https://zeustracker.abuse.ch/index.php

One enterprise strategy for combatting Zeus/SpyEye malware infections has been to track known C2 servers and block outgoing connections to these servers and/or blackhole DNS requests to associated domains. So Zeus/SpyEye has created another industry– threat intelligence services that find and track C2 servers, and enterprise security vendors that sell subscription feeds and COTS devices to integrate with existing security infrastructures.

At any given moment there are dozens of known Zeus/SpyEye C2 servers in operation all over the world. A surprising number are in jurisdictions which are accessible to Western authorities. This may be do to low prices and availability of bandwidth.



But tracking these C2 servers can be a difficult task. Systems infected with the Zeus/SpyEye trojan can be used as web proxies. Bot masters select their fastest infected machines to act as relays between bots and the actual C2 infrastructure. Relays are constantly moved in and out of so called "fast flux" domains making it difficult for researchers to track back to the actual C2 infrastructure servers.

Careful bot masters will force relay connections through multiple competing or unfriendly jurisdictions and may locate the actual servers where Western authorities cannot reach them.

Even if one C2 infrastructure is found and disrupted, "bullet proof" hosting arrangements guarantee that the server will be up and running at a new location within 24hrs or less. This is an unending game of "whack-a-mole".

And the appearance of the "Game Over" variant now means that there is no centralized C2 infrastructure to disrupt. There is now only a sea of infected machines, any one of which can provide instructions and updates to its peers.

I have no product to sell you and no wish to spread fear, uncertainty, and doubt. But it is true that the ready availability of powerful COTS tools like Zeus and SpyEye have created a business opportunity and an underground economy that rivals many of the world's fastest growing nations.

And in the face of increasing globalization, there are still many places in the world where economic opportunity is unavailable– whether due to lack of infrastructure, official corruption, or some other reason. Ask yourself, if you were given a choice between committing a crime against citizens of a country halfway around the world from you and being able to feed and shelter your family and make a better life for them, which would you choose?

Industrialized nations are disproportionally at risk to these kinds of attacks due to our dependence on networked technologies. As has been well documented by others, the technologies we used were designed to facilitate information sharing, and not always to protect and safeguard that information. Our electronic defenses are a patchwork of band-aid solutions that leave as many holes as they cover.

We face an adaptive, motivated opponent who recognizes that they do not have to go after difficult targets. Instead, like any predator, they fatten on the weakest members of the heard. And unlike the real world, this process of natural selection does not make the rest of the heard stronger, but rather weakens everybody.