threatpost

The Kaspersky Lab Security News Service

Spotlight Series

Threatpost's Top Security News Stories of 2011

Featured Articles:

It was a year that began with rabid and ceaseless speculation about the origins of Stuxnet and ended with equally breathless conjecture about the SCADA-munching worm's putative cousin, Duqu. Along the way, the steady drumbeat of data breaches nailing major global enterprises (Sony, Citibank, Disney) continued unabated.

Little known hacker collaborative such as LulzSec and Anonymous grew up to become household names and major players on the international political scene. Meanwhile the major vendors we rely on to develop and maintain secure technology products -- Microsoft, Google, Apple, et al – saw weaknesses in their wares turned against them, and the rest of us, with alarming frequency. Such is the state of cyber insecurity in 2011.

It's our duty and our pleasure here at Threatpost to chronicle the sometimes maddening, often chaotic, always interesting events in security. For good or for ill, every story that affects the safety and integrity of data and technology assets affects global commerce and the lives of all who rely on it. That means all of us. Heady stuff.

So, as the year draws to a close, we've compiled our list of the Top Security Stories of 2011, presented here in no particular order. These are the issues that shook the world's markets and kept us awake at night. If there's a lesson here, it's that cybersecurity challenges aren't going away anytime soon. In fact, as we look forward to 2012, about the only thing that could quell the continuing battle to secure technology system is if the Mayans turn out to be right.

And none of us is rooting for that.

Enjoy!

Stuxnet Finger Pointing

Stuxnet debuted with a frenzy in 2010 after researchers exposed the malware already busily disrupting Iran's nuclear enrichment program. That was followed this past year by continued speculation, finger pointing and even some dismissive attitudes about the worm, which targets Siemens-made industrial control devices. The most troubling buzz of 2011 was that many of the vulnerabilities exploited by Stuxnet remain unpatched. Not to worry, say some experts. Nobody has stepped forward to take credit for crafting the disruptive worm, and for good reason, they say. Basic errors in the original Stuxnet code made the malware less effective and easier to detect than it might have been. The mistakes likely also mean that the programmers behind the Stuxnet attack may not have been the super-elite cadre of state-sponsored developers we've been led to believe.

Many Stuxnet Vulnerabilities Still Unpatched

By Paul Roberts

The media storm over the Stuxnet worm may have passed, but many of the software holes that were used by the worm remain unpatched and leave Siemens customers open to a wide range of potentially damaging cyber attacks, according to industrial control system expert Ralph Langner.

Writing on his personal blog, Langner said that critical vulnerabilities remain in Windows-based management applications and software used to directly manage industrial controllers by Siemens Inc., whose products were targeted by the Stuxnet worm.

Siemens did not immediately respond to a request for comment on Langner's statement.

Langner, a principal and founder of Langner Communications GmbH is an independent expert on industrial control system security. He was among the first to connect the Stuxnet worm to an attack on uranium enrichment facilities within Iran. He was also among those who pinned responsibility for the attack on the United States and Israel.

Langner's company sells security software and services to firms in the industrial control field. In the past, he has been critical of both the media coverage of the Stuxnet worm and of Siemens response to revelations that software vulnerabilities and other structural weaknesses in its products contributed to the creation of Stuxnet and the success of the attack.

Writing on his blog on Tuesday, Langner said that the media paid too much attention to the four, zero day Windows vulnerabilities that enabled the Stuxnet worm, but overlooked the other security holes used by the worm. Unlike the Windows vulnerabilities, which Microsoft quickly fixed, many of the holes in Siemens' products remain unpatched, he contends.

Langner enumerates three types of exploits used by Stuxnet - only one category of which (Windows operating system exploits) have been closed. The other two are Windows applications exploits aimed at Siemens Simatic Manager and the Siemens WinCC SCADA application, and controller exploits aimed at Siemens S70-300 and 400 series controllers.

In the case of the Siemens Windows-based management software, attackers could use a combination of strategies to compromise these vulnerable components, including a hard coded password in the WinCC product that was leveraged by Stuxnet. Siemens famously advised customers not to change that password out of fear that doing so would disrupt communications between WinCC and its back end database. Langner says that Stuxnet combined the hard coded password backdoor with SQL injection attacks to compromise systems running WinCC. Without a software fix, other attackers could also follow in Stuxnet's footsteps: hijacking a Siemens driver or tricking the software to run arbitrary code placed in engineering folders used by the products.

Even more serious are unpatched and exploitable vulnerabilities on the controllers themselves. Langner said this category of vulnerability "opens the door to extremely aggressive attacks that do not have to be nearly as surgical as it (sp) was seen in Stuxnet."

Stuxnet has provided a model that less sophisticated hackers can copy in future attacks. Attackers could, for example, learn from Stuxnet which code to insert into the vulnerable controller to freeze it in its current operating state. Such an attack would be hard to detect and require little knowledge of how the Siemens S7 controllers actually work. Fixing the holes is also difficult, because they are considered "features" of the Siemens controllers, rather than security holes, Langner said.

Siemens customers have few choices to protect vulnerable installations. One is to use white listing technology to prevent unauthorized applications from running on the systems that are also running the Siemens software. However, firms using industrial control systems haven't necessarily purchased white listing tools, and not all whitelisting products recognize and support the Siemens applications.

Beyond that, Langner said Siemens should update its industrial control products to recognize and support digitally signed code, preventing rogue attack code from being run by the devices.

Long overlooked by malicious hackers, firms manag-

ing critical infrastructure and the vendors that serve that market now find themselves in the cross hairs of security researchers, as well as sophisticated cybercriminal groups and nation-state sponsored hackers. Both have been buffeted by reports of serious security holes in recent years that revealed a laissez faire attitude towards IT security.

To that point, Langner said that even the patched Windows holes could be used to attack Siemens customers. Exploits for those holes are now part of commonly available penetration testing tools like Metasploit and Canvas, and its likely that some Siemens customers have applied the patches to vulnerable systems. Siemens customers should be very concerned about attacks and warned against the complacency that might result from coverage of Stuxnet's uniqueness and complexity.

"Operation Myrtus required one or two geniuses to design Stuxnet," he warns. "Understanding and copying the design can be achieved by average engineers. Even worse, the design AND PRODUCTION process can be packaged into a software tool , enabling immoral idiots and geniuses alike to configure highly aggressive cyber weapons."

Stuxnet Authors Made Several Basic Errors

By Dennis Fisher

ARLINGTON, VA--There is a growing sentiment among security researchers that the programmers behind the Stuxnet attack may not have been the super-elite cadre of developers that they've been mythologized to be in the media. In fact, some experts say that Stuxnet could well have been far more effective and difficult to detect had the attackers not made a few elementary mistakes.

In a talk at the Black Hat DC conference here Tuesday, Tom Parker, a security consultant, presented a compelling case that Stuxnet may be the product of a collaboration between two disparate groups, perhaps a talented group of programmers that produced most of the code and exploits and a less sophisticated group that may have adapted the tool for its eventual use. Parker analyzed the code in Stuxnet and looked at both the quality of the code itself as well as how well it did what it was designed to do, and found several indications that the code itself is not very well done, but was still highly effective on some levels.

Parker wrote a tool that analyzed similarities between the Stuxnet code and the code of some other well-known worms and applications and found that the code was fairly low quality. However, he also said that there was very little chance that one person could have put the entire attack together alone.

"There are a lot of skills needed to write Stuxnet," he said. "Whoever did this needed to know WinCC programming, Step 7, they needed platform process knowledge, the ability to reverse engineer a number of file formats, kernel rootkit development and exploit development. That's a broad set of skills. Does anyone here think they could do all of that?"

That broad spectrum of abilities is what has led many analysts to conclude that Stuxnet could only be the work of a well-funded, highly skilled group such as an intelligence agency or other government group. However, Parker pointed out that there were a number of mistakes in the attack that one wouldn't expect to find if it was launched by such an elite group. For example, the command-and-control mechanism is poorly done and sends its traffic in the clear and the worm ended up propagating on the Internet, which was likely not the intent.

"This was probably not a western state. There were too many mistakes made. There's a lot that went wrong," he said. 'There's too much technical inconsistency. But, the bugs were unlikely to fail. They were all logic flaws with high reliability."

Parker said that Stuxnet may have been developed originally on contract and then once it was handed off to the end user, that group adapted it by adding the C&C infrastructure and perhaps one of the exploits, as well.

The mistakes weren't limited to the operational aspects of Stuxnet, either. Nate Lawson, a cryptographer and expert on the security of embedded systems, said in a blog post Monday that the Stuxnet authors were very naive in the methods they used to cloak the payload and target of the malware. Lawson said that the Stuxnet authors ignored a number of well-known techniques that could have been much more effective at hiding the worm's intentions.

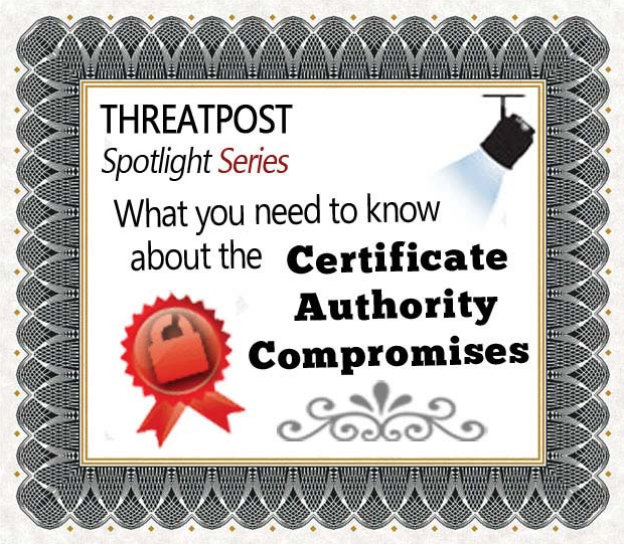
"Rather than being proud of its stealth and targeting, the authors should be embarrassed at their amateur

approach to hiding the payload. I really hope it wasn't written by the USA because I'd like to think our elite cyberweapon developers at least know what Bulgarian teenagers did back in the early '90s," Lawson said. "First, there appears to be no special obfuscation. Sure, there are your standard routines for hiding from AV tools, XOR masking, and installing a rootkit. But Stuxnet does no better at this than any other malware discovered last year. It does not use virtual machine-based obfuscation, novel techniques for anti-debugging, or anything else to make it different from the hundreds of malware samples found every day."

Lawson concludes that whoever wrote Stuxnet likely was constrained by time and didn't think there was enough of a return to justify the investment of more time in advanced cloaking techniques.

Hackers Take Center Stage

After a decade of flourishing unseen in the shadows of the Internet, Anonymous, LulzSec and other like-minded groups expanded their activities from obscure attacks and protests to full fledged hacking and DDoS campaigns against governments, The Church of Scientology, Visa, Paypal, Sony and a wide range of other private and public organizations perceived as hostile to the hackers' ever shifting list of pet causes. Among the defining events of 2001's hacker evolution came when Aaron Barr, CEO of security consulting firm and government contractor HBGary Federal was forced to step down after his public taunting of Anonymous led to an embarrassing data breach. Hackers broke into HBGary's computer network and published tens of thousands of company email messages on the Internet. The attack even caused HBGary to bail out of February's RSA conference in an effort to limit the PR damage.



Teens, Lulz and Morality: Making Sense of Anonymous

By Paul Roberts

The UK's Metropolitan Police swooped down on the remote, weather beaten Shetland Islands last week to arrest what the authorities claim is a top ranking member of the international hacker collective Anonymous, which has been terrorizing governments and high profile corporations for most of the last six months. The arrest of Jake Davis, aka "Topiary" capped a busy month for law enforcement in the U.S. and U.K., with raids on dozens of homes and the arrest of reputed leaders of both Anonymous and the affiliated Lulz Security, including Marshall Webb, the Ohio man known online as "m_nerva," Ryan Cleary, the alleged botnet operator known as "Ryan," and a fellow Brit known online as "Tflow."

The details of the cases against these men haven't yet been presented and their innocence, of course is presumed. What's known about them, publicly, is anecdotal. But what is clear is that they're all young. Webb and Cleary: 19, Davis 18, and the minor known as Tflow reportedly just 16. Presuming the evidence against them holds up, should we be surprised to find the faces of adolescents staring out at us from behind the Guy Fawkes masks? History and science say: "no."

More than a decade of psychological, medical and scientific research suggest that adolescents are particularly susceptible to the kinds of risky, spontaneous and harmful attacks that became Anonymous's hallmark. The question for the security community - and for society - is how to stop it from happening again.

The stereotype of the brilliant but socially isolated hacker-teen has gone hand in hand with society's awareness of computer hacking itself. Look no further than seminal Hollywood films like Wargames (1983) or Hackers (1995) for that. In recent years, however, there's been a concerted effort to dispel that myth. The media (including yours truly) have written time and again about the professionalization of malware

writing and cyber crime. Criminal syndicates took over the business of creating, releasing and monetizing malicious software, so the story goes. Cybercrime became a vertical industry with specialties, sub-specialties and lots of money. Finally, nation and nation-backed actors got into the cyber game, with a focus on espionage and control of critical infrastructure. The days of the hobbyist hacker were gone - or at least that's what we thought.

Of course, that was never the whole story. In the last decade, Anonymous and other like-minded groups flourished in the shadows of the Internet: amorphous and anarchic collectives that congregated on IRC and on image boards like 4Chan. What eventually became known as "Anonymous" was born in that freewheeling, no-holds-barred world, then inexorably expanded its activities from obscure attacks and protest actions to full fledged hacking and DDoS campaigns against governments, The Church of Scientology, Visa, Paypal, Sony and a wide range of other private and public organizations perceived as hostile to Anonymous's ever shifting list of pet causes.

The advent of Anonymous, Lulz Security and similar groups remind us that hacking for laughs - or "lulz" - never went away. It only faded into the background. But we shouldn't have been surprised. Indeed, none of the underlying trends that draw smart, technically adept young men (mostly) and women to malicious hacking have abated. To the contrary, changes in the computing environment have put even more firepower into the hands of would-be hackers. Anonymous's frequent use of free services like YouTube, pastebin, the Low orbit Ion Cannon distributed denial of service (DDoS) software and other tools make clear how free and Web-based tools and technologies make it possible to communicate, coordinate and carry out potent online attacks anonymously. And, as has always been the case, the particular "condition" of adolescents puts them at risk for gravitating to this type of activity.

Early studies, such as Sarah Gordon's work on the psychology of hackers and virus writers, found a correlation between adolescents and both hacking and virus writing, but made a distinction between adolescents who might engage in those behaviors and their older colleagues. The youths, Gordon found, were motivated by social and intellectual challenges: solving a puzzle and an age appropriate desire to rebel and gain credibility with peers, feel special or get "famous." Adults engaged in the same activities, Gordon found, fit the more standard psychological profile of criminals.

The latest scientific research tends to back up Gordon's findings. New brain imaging studies show that the brain undergoes dramatic change during adolescence. Because of this, adolescents, are less able to employ empathy in helping to make decisions, according to studies.

Other research shows that the cerebellum, which coordinates our cognitive processes -- our mental grace, if you will -- changes dramatically throughout adolescence and into one's early 20s. Finally, teens, though adult-seeming, are still in the process of socializing. By and large, they socialize by observing the behavior of those around them - conducting a type of "social learning" that goes on throughout life, but especially during youth and adolescence. No surprise, then, that hours spent online with groups that include adults or trusted friends who are inclined towards criminal behavior might just help to normalize that behavior for an adolescent.

What does this tell us about the teenagers who found themselves with their finger on the trigger Anonymous's LOIC DDoS cannon? Nothing and everything. It's long been clear that Anonymous's claims to be "leaderless" were just posturing. We'll have to wait for the courts and attorneys to help us understand the real actions and motivations of those who carried

out the attacks against HBGary Federal, Sony and other organizations - who was the general and who was the loyal foot soldier.

However, reporters who have covered the group's exploits and winced at the ruthlessness of attacks on individuals like Aaron Barr won't be surprised that the individuals behind faceless personas like "Topiary" and "Tflow" hadn't seen the other side of 20. The juvenile banter, unquenchable thirst for attention (press or otherwise) and prank playing all screamed "teenager," even as members of the group projected an air of adult confidence and righteous indignation in the press. Just underneath all the posturing, however, lay the kind of dangerous moral disengagement that researchers long ago spotted in adolescent hackers and virus writers and the cocktail of dissociative effects that go along with online relationships - what one researcher has termed the "online disinhibition effect." These factors made it easy enough for Anonymous and Lulz Security's leadership to cook up easy and comfortable justification for their malicious acts. "He was out to get us. " "Their security was a joke." "They're hostile to a cause we support." "They deserved it." Judging from the text of the leaders' IRC chats, the prospect of getting caught and arrested wasn't alien, though it's almost certain that the reality of that is more sobering than the theory of it.

The moral of Anonymous may be that, in the end, the group's slogan - "we are legion" - wasn't that far off after all. The flurry of arrests in recent months suggest that Anonymous did have a healthy following who, if not legion, were at least numerous. Indeed,the particularities of adolescence almost guarantee a willing and wired population of followers who might easily be swayed to join in the fun.

We in the media, however, didn't do a good job spotting the juvenilia and seeing it for what it was. All our talk about Chinese hackers, mobsters and "advanced persistent threats" had us swallowing Anonymous's line that they were latter day Robin Hoods out to expose the wickedness in the Beltway and the board room. There may be something to that, but they were also teenagers huddled away in the basement and the bedroom with their laptop and a broadband connection.

As a community, we need to pick up the threads of that conversation we collectively dropped almost a decade ago, asking ourselves what factors -social, psychological, economic - might draw smart, young people into groups such as Anonymous and LulzSec that, in the end, were bent on committing illegal acts. Once we can answer those questions, it becomes easier to figure out what steps - be they education or outreach - might prevent the next iteration of Anonymous, Lulz Security or Antisec from finding its feet.

HBGary Federal CEO Aaron Barr Steps Down

By Paul Roberts

Embattled CEO Aaron Barr says he is stepping down from his post at HBGary Federal to allow the company to move on after an embarrassing data breach.

The announcement comes three weeks after Barr became the target of a coordinated attack by members of the online mischief making group Anonymous, which hacked into HBGary Federal's computer network and published tens of thousands of company e-mail messages on the Internet. HBGary did not respond to telephone and e-mail requests for comments on Barr's resignation.

In an interview with Threatpost, Barr said that he is stepping down to allow himself and the company he ran to move on in the wake of the high profile hack.

"I need to focus on taking care of my family and rebuilding my reputation," Barr said in a phone interview. "It's been a challenge to do that and run a company. And, given that I've been the focus of much of the bad press, I hope that, by leaving, HBGary and HBGary Federal can get away from some of that. I'm confident they'll be able to weather this storm."

Anonymous conducted a preemptive strike on HBGary after Barr was quoted in a published article saying that he had identified the leadership of the group and planned to disclose their identities at the B-Sides Security Conference in San Francisco. By combining a SQL injection attack on HBGary's Web site with sophisticated social engineering attacks, the group gained access to the company's Web- and e-mail servers as well as the Rootkit.com Web site, a site also launched by HBGary founder Greg Hoglund. Ultimately, the group defaced HBGary's Web site and disgorged the full contents of e-mail accounts belonging to Barr, Hoglund and other company executives.

Though Barr and HBGary were the victims of the hack, the contents of the e-mail messages divulged plans

that cast both in an unflattering light. HBGary counted many U.S. government agencies, including the Department of Defense, CIA and NSA as customers. The disclosure of e-mail messages from the company poses a major security risk to those organizations, as well as individuals who had corresponded with the firm. The breach also raises troubling questions about the direction that HBGary and other Beltway firms have taken. Email exchanges published online revealed the firm to be at work on a variety of plans to do data mining and information operations on U.S. organizations and journalists on behalf of clients including law firms representing a large U.S. bank and the U.S. Chamber of Commerce. Most recently, the incident spilled into the mainstream, with comedian Stephen Colbert devoting a segment of his Colbert Report program on February 24 to the HBGary hack.

RSA 2011: Winning the War But Losing Our Soul

By Paul Roberts

There was lots of noise and distraction on the crowded Expo floor of the RSA Security Conference this year. After a grueling couple of years, vendors were back in force with big booths, big news and plenty of entertainment designed to attract visitor traffic. Wandering the floor, I saw - variously - magic tricks, a man walking on stilts, a whack-a-mole game, a man dressed in a full suit of armor and a 15 foot long racetrack that I would have killed for when I was 10.

The most telling display, however, may have been the one in Booth 556, where malware forensics firm HBGary displayed a simple sign saying that it had decided to remove its booth and cancel scheduled talks by its executives. This, after the online mischief making group Anonymous broke into the computer systems of the HBGary Federal subsidiary and stole proprietary and confidential information. The HBGary sign stayed up for a couple days, got defaced by someone at the show and was later removed. When I swung by HBGary's booth on Thursday, it was a forlorn and empty patch of brown carpet where a couple marketing types where holding an impromptu bull session.

It would be easy to say that the lesson of HBGary is that "anyone can get hacked." After all, the company's founder, Greg Hoglund is one of the smartest security folks around - hands down. He's a recognized expert on malware and, literally, wrote the book on rootkit programs. HBGary Federal's customers included the U.S. Department of Defense as well as spy agencies like the CIA and NSA.

Or maybe the lesson of HBGary is simply not to "kick the hornet's nest," so to speak: needlessly provoking groups like Anonymous who have shown themselves to be hungry for publicity and have little to lose in a confrontation. Maybe, the lesson is simply that, if you're going to kick the hornet's nest, as HBGary Federal CEO Aaron Barr was determined to, then at least to spend some time securing your Web- and e-mail infrastructure and following password security best practices before you commence said kicking.

But I think the real lesson of the hack - and of the revelations that followed it - is that the IT security industry, having finally gotten the attention of law makers, Pentagon generals and public policy establishment wonks in the Beltway, is now in mortal danger of losing its soul. We've convinced the world that the threat is real - omnipresent and omnipotent. But in our desire to combat it, we are becoming indistinguishable from the folks with the black hats.

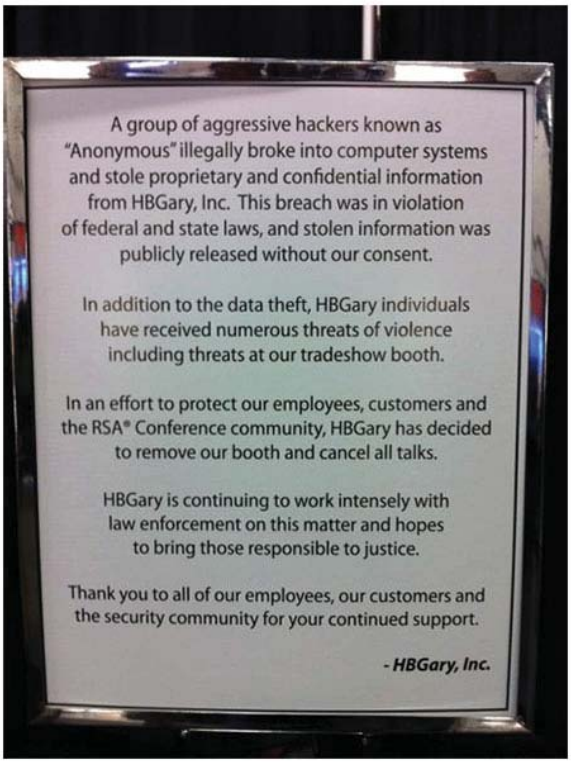
Of course, none of this is intended to excuse the actions of Anonymous, who HBGary President Penny Leavy, in a conversation with Threatpost, rightly labeled "criminals" rather than politically motivated "hacktivists." The attack on HBGary was an unsubtle, if effective, act of intimidation designed to send a message to Barr and other would be cyber sleuths: 'stay away.'

We can see their actions for what they are, and sympathize deeply with Aaron Barr, Greg Hoglund and his wife (and HBGary President) Penny Leavy for the harm and embarrassment caused by the hackers from Anonymous, who published some 70,000 confidential company e-mails online for the world to see. Those included confidential company information, as well as personal exchanges between HBGary staff that were never intended for a public airing. Its easy to point the finger and chortle upon reading them, but how many of us (or the Anonymous members, themselves) could stand such scrutiny?

Its harder to explain away the substance of many other

e-mail messages which have emerged in reporting by Ars Technica as well as others. They show a company executives like HBGary Federal CEO Aaron Barr mining social networks for data to "scare the s***" out of potential customers, in theory to win their business. While "scare 'em and snare 'em" may be business as usual in the IT security industry, other HBGary Federal skunk works projects clearly crossed a line: a proposal for a major U.S. bank, allegedly Bank of America, to launch offensive cyber attacks on the servers that host the whistle blower site Wikileaks. HBGary was part of a triumvirate of firms that also included Palantir Inc and Berico Technologies, that was working with the law firm of the U.S. Chamber of Commerce to develop plans to target progressive groups, labor unions and other left-leaning non profits who the Chamber opposed with a campaign of false information and entrapment. Other leaked e-mail messages reveal work with General Dynamics and a host of other firms to develop custom, stealth malware and collaborations with other firms selling offensive cyber capabilities including knowledge of previously undiscovered ("zero day") vulnerabilities.

Look, there's nothing wrong with private firms helping Uncle Sam to develop cyber offensive capabilities. In an age of sophisticated and wholesale cyber espionage by nation states opposed to the U.S., the U.S. government clearly needs to be able to fight fire with fire. Besides, everybody already knew that Greg Hoglund was writing rootkits for the DoD, so is it right to say we're "shocked! shocked!" to read his e-mail and find out that what we all suspected was true? I don't think so.



What's more disturbing is the way that the folks at HBGary - mostly Aaron Barr, but others as well - came to view the infowar tactics they were pitching to the military and its contractors as applicable in the civilian context, as well. How effortlessly and seamlessly the focus on "advanced persistent threats" shifted from government backed hackers in China and Russia to encompass political foes like ThinkProgress or the columnist Glenn Greenwald. Anonymous may have committed crimes that demand punishment - but its up to the FBI to handle that, not "a large U.S. bank" or its attorneys.

The HBGary e-mails, I think, cast the shenanigans on the RSA Expo floor in a new and scarier light. What other companies, facing the kind of short term financial pressure that Barr and HBGary Federal felt might also cross the line - donning the gray hat, or the black one? What threat to all of our liberties does that kind of IT security firepower pose when its put at the behest of corporations, government agencies, stealth political groups or their operatives? Bruce Schneier - our industry's Obi-Wan Kenobi - has warned about this very

phenomena: the way the military's ever expanding notion of "cyber war," like the Bush era's "War on Terror" does little to promote security, but a lot to promote inchoate fear. That inchoate fear then becomes a justification for further infringement on our liberties.

"We reinforce the notion that we're helpless -- what person or organization can defend itself in a war? -- and others need to protect us. We invite the military to take over security, and to ignore the limits on power that often get jettisoned during wartime," Schneier observed. That kind of conflation is clear reading Barr's e-mails where the line between sales oriented tactics and offensive actions blur. The security industry veterans I spoke with at this year's show were as aghast at Barr's trip far off reservation, but they also expressed a weary recognition that, in the security business, this is where things are headed.

What's the alternative? Schneier notes that focusing on cyber crime as "crime" rather than "war" tends to avoid the problems with demagoguery. Focus on cyber crime and hacking in the same way as you focus on other types of crimes: as long term problems that must be managed within the "context of normal life," rather than "wars" that pose an existential threat to those involved and must be won at all costs. The U.S. needs peacetime cyber-security "administered within the myriad structure of public and private security institutions we already have" rather than extra-judicial vigilantism and covert ops of the kind the HBGary e-mails reveal. Here's hoping HBGary is the wake up call the industry needed to reverse course.

Data Breaches for All

Sony's online gaming platform, The PlayStation Network (PSN), disappeared for more than a month starting in April, and no amount of double X and O-ing or right joysticking could save it. The reason? A massive attack on PSN's network knocked the gaming giant offline and exposed the data of more than million users worldwide. The system was brought back online at the end of May, but the company was left with $170 million in clean-up costs and few solid leads regarding the perpetrators. Speculation has run the gamut, from Anonymous hackers to disgruntled ex-employees.

While Sony quietly struggled to get PSN back online, most of the security community remained abuzz with news that massive online marketing firm Epsilon had exposed the customer data of unknown millions of end users doing businesses with just about every major corporation in the Western world. From Capitol One to Citibank to Disney, few were immune to data breaches in 2011.

Playstation Network Down Following 'External Intrusion'

By Brian Donohue

Sony's online gaming platform, The PlayStation Network (PSN), continued a five day outage on Monday after what the company described as an "attack" on its network knocked PSN offline on April 20. And hope is fading for a fast resolution, with Sony saying it is revamping the network to make it more secure. The company released a statement on their PlayStation blog on Friday claiming that an "external intrusion on our systems has affected our PlayStation Network and Qriocity services." The company said PSN has been turned off, and will remain off, until Sony is satisfied that their network is secure enough that this sort of thing won't happen in the future.

While Sony did not attribute blame for the attack, published reports have speculated that the online mischief-making collective, Anonymous, might be behind the hack of Qriocity, a media streaming service that was hosted on the PlayStation Network. The group has claimed responsibility for denial of service attacks against Sony for legal attacks on hacker enthusiasts who have cracked content protection technology for its PS3 and other products.

On Friday, Anonymous posted a statement on the Web site Anonnews.org denying responsibility for the hack. "For once, we didn't do it," the statement read.

In a post at PlayStation's self-help Knowledge Center, the gaming giant claims they are working around the clock to bring the network and Qriocity, their music and movie streaming service, back online. Unfortunately for a number of increasingly destitute gamers, there is little hope that the PSN will return to service anytime soon, as PlayStation says they are in the pro-

cess of "rebuilding [their] system to strengthen [their] network infrastructure."

Revelations that this outage was likely the result of an external attack aren't altogether surprising considering the amount of ire Sony has drawn from the hacking community as a result of their legal action against suspected PS3 hackers.

Epsilon Data Breach Expands to Include Capital One, Disney, Others

By Dennis Fisher

The compromise of a system at online marketing company Epsilon Data Management that came to light last week and involves the email addresses and names of customers at companies such as Citibank, Kroger and Disney expanded over the weekend to include a slew of other companies. The attack does not appear to have compromised any customer financial data or other sensitive information.

Word of the attack on Epsilon began to filter out last week when a handful of companies began notifying their customers that their email addresses and perhaps their names were compromised. Then on Friday Epsilon posted a terse notice about the attack on its system.

"On March 30th, an incident was detected where a subset of Epsilon clients' customer data were exposed by an unauthorized entry into Epsilon's email system. The information that was obtained was limited to email addresses and/or customer names only. A rigorous assessment determined that no other personal identifiable information associated with those names was at risk. A full investigation is currently underway," the statement said.

The first companies began notifying customers of the attack late last week, including Kroger and others. In the last couple of days more and more companies have sent out notifications as well, including some very large retailers, such as Walgreen's and the credit card company Capital One.

One such letter, from Disney Destinations, warns customers that their information has been compromised and that they may end up seeing more spam as a result.

"We have been informed by one of our email service providers, Epsilon, that your email address was exposed by an unauthorized entry into that provider's computer system. We regret that this incident has occurred and any inconvenience this incident may cause you. We take your privacy very seriously, and we will continue to work diligently to protect your personal information," the statement says.

"We want to assure you that your email address was the only personal information we have regarding you that was compromised in this incident. As a result of this incident, it is possible that you may receive spam email messages, emails that contain links containing computer viruses or other types of computer malware, or emails that seek to deceive you into providing personal or credit card information."

Other companies that have reported that their customers are affected by the Epsilon breach include Home Shopping Network, JP Morgan Chase and TiVo.

Epsilon is a major email marketing firm that sends messages to end users on behalf of its roster of corporate clients. The company claims to be the largest opt-in marketing company, sending 40 billion messages every year.

Microsoft's Perennial Vulnerability

No annual list of security concerns would be complete without a rundown of the ways Microsoft dropped the ball along the way. In fairness, the vendor's security efforts have greatly improved in the past decade, but challenges remain for the Redmondians. For example: The year began with Microsoft warning users about a dangerous flaw in the way its Windows OS handles MHTML, which could allow an attacker to run malicious scripts on vulnerable machines. The bug affects all of the current versions of Windows, from XP up through Windows 7 and Windows Server 2008. Then in August, a new worm dubbed Morto began infecting servers and workstations via Microsoft's proprietary Remote Desktop Protocol. Users reported that Morto was infecting completely patched machines running clean installations of Win-

dows Server 2003. To make matters worse, in November, Microsoft was scrambling to close holes in Windows 7 and Vista that allowed a rootkit known as TDL4 to bypass Windows' own driver-signing protections.

Microsoft Warns of MHTML Bug in Windows

By Dennis Fisher

Microsoft is warning its users about a dangerous flaw in the way that Windows handles certain MHTML operations, which could allow an attacker to run code on vulnerable machines. The bug affects all of the current versions of Windows, from XP up through Windows 7 and Windows Server 2008.

Microsoft issued an advisory about the MHTML vulnerability, which has been discussed among security researchers in recent days. There is some exploit code available for the bug, as well. In addition to the advisory, Microsoft has released a FixIt tool, which helps mitigate attacks against the vulnerability in Windows.

"The vulnerability could allow an attacker to cause a victim to run malicious scripts when visiting various Web sites, resulting in information disclosure. This impact is similar to server-side cross-site scripting (XSS) vulnerabilities. Microsoft is aware of published information and proof-of-concept code that attempts to exploit this vulnerability. At this time, Microsoft has not seen any indications of active exploitation of the vulnerability," the company said in the advisory.

"The vulnerability exists due to the way MHTML interprets MIME-formatted requests for content blocks within a document. It is possible under certain conditions for this vulnerability to allow an attacker to inject a client-side script in the response of a Web request run in the context of the victim's Internet Explorer. The script could spoof content, disclose information, or take any action that the user could take on the affected Web site on behalf of the targeted user."

The FixIt workaround that Microsoft released for the MHTML vulnerability enables the Network Protocol Lockdown in Internet Explorer for all of the security zones. The side effects from enabling the FixIt workaround are minor, Microsoft officials said.

"In our testing, the only side effect we have encountered is script execution and ActiveX being disabled within MHT documents. We expect that in most environments this will have limited impact. While MHTML is an important component of Windows, it is rarely used via mhtml: hyperlinks. Most often, MHTML is used behind the scenes, and those scenarios would not be impacted by the network protocol lockdown. In fact, if there is no script content in the MHT file, the MHT file would be displayed normally without any issue. Finally, for legitimate MHT files with script content that you would like to be rendered in IE, users can click the information bar and select "Allow All Protocols"," the company said.

New Worm Morto Using RDP to Infect Windows PCs

By Dennis Fisher

A new worm called Morto has begun making the rounds on the Internet in the last couple of days, infecting machines via RDP (Remote Desktop Protocol). The worm is generating a large amount of outbound RDP traffic on networks that have infected machines, and Morto is capable of compromising both servers and workstations running Windows.

Users who have seen Morto infections are reporting in Windows help forums that the worm is infecting machines that are completely patched and are running

clean installations of Windows Server 2003.

"In a new windows 2003 R2 server, I'm noticing every few minutes, svshost.exe [sic] is opening a ton of outgoing TCP 3389 connections. I ran an a/v scanner over it and it's clean. Can it be hacked already??? has anyone seen this before?," one user asked in Microsoft's TechNet forum.

On Sunday, the SANS Internet Storm Center reported a huge spike in RDP scans in the last few days, as infected systems have been scanning networks and remote machines for open RDP services. One of the actions that the Morto worm takes once it's on a new machine is that it scans the local network for other PCs and servers to infect.

"A few weeks ago a diary posted by Dr. J pointed out a spike in port 3389 traffic. Since then the sources have spiked ten fold. This is a key indicator that there is an increase of infected hosts that are looking to exploit open RDP services." SANS handler Kevin Shortt said in a blog post.

Researchers at F-Secure said that Morto is the first Internet worm to use RDP as an infection vector. Once it's on a new machine and has successfully found another PC to infect, it starts trying a long list of possible passwords for the RDP service.

"Once a machine gets infected, the Morto worm starts scanning the local network for machines that have Remote Desktop Connection enabled. This creates **a lot of traffic for port 3389/TCP**, which is the RDP port," F-Secure Chief Research Officer Mikko Hypponen said in a blog post.

"Once you are connected to a remote system, you can access the drives of that server via Windows shares like **\\tsclient\c** and **\\tsclient\d** for drives **C:** and **D:**, respectively. Morto uses this feature to copy itself to the target machine. It does this by creating a temporary drive under letter A: and copying a file called **a.dll** to it. The infection will create several new files on the system including **\windows\system32\sens32.dll** and **\windows\offline web pages\cache.txt**. Morto can be controlled remotely. This is done via several alternative servers, including **jaifr.com** and **qfsl.net**."

It's been quite a while since there was a large-scale Internet worm attack. Once upon a time, worms such as Blaster, Code Red and SQL Slammer were all the rage and found success clogging networks with enormous amounts of scanning traffic and other activity. But those kinds of events have become an anachronism as attackers have turned the attention to for-profit attacks.

Think Safer

Not even a techno-religion is immune from security snafus, as the folks at Apple are steadily discovering. After years of watching the bad guys use crimeware kits like Zeus against Microsoft, the iGang finally got a malware construction tool to call its own in May of this year. Modeled on the ubiquitous Zeus, the new Apple OS X crimeware kit consists of a builder, an admin panel, encryption support, and the ability to steal browser forms, according to the Danish researchers at CSIS, who first encountered the malware tool. And if that wasn't enough, in July, security researcher and Apple expert Charlie Miller found a way to completely disable the batteries on Apple laptops, making them permanently unusable. The method, which involves accessing and sending instructions to the processor and firmware resident on Apple's "smart" batteries, could also be used for more malicious purposes down the road, Miller warned.

Crimeware Kit Emerges for Mac OS X

By Dennis Fisher

Crimeware kits have become a ubiquitous part of the malware scene in the last few years, but they have mainly been confined to the Windows platform. Now, reports are surfacing that the first such kit targeting Apple's Mac OS X operating system has appeared.

The kit is being compared to the Zeus kit, which has been one of the more popular and pervasive crimeware kits for several years now. A report by CSIS, a Danish security firm, said that the OS X kit uses a template that's quite similar to the Zeus construction and has the ability to steal forms from Firefox.

"The Danish IT-security company CSIS Security Group has just yesterday observed a new advanced Form grabber designed for the Mac OS X operating system being advertised on several closed underground forums. In the same way as several other DIY crimeware kits designed for PCs, this tool consists of a builder, an admin panel and supports encryption," Peter Kruse of CSIS said in a blog post.

"The kit is being sold under the name Weyland-Yutani BOT and it is the first of its kind to hit the Mac OS platform. Apparently, a dedicated iPad and Linux release are under preparation as well. The Weyland-Yutani BOT supports web injects and form grabbing in Firefox; however both Chrome and Safari will soon follow. The webinjects templates are identical to the ones used in Zeus and Spyeye."

In an email exchange, Kruse said that the builder component of the kit runs on Windows machines and the user has the option of specifying that he wants the malware to run on OS X. The builder will then create a Mac binary.

Malware authors and professional attack crews have steered clear of the OS X platform for the most part, for a variety of reasons. One of the main things holding up the development of Mac-specific attack tools, experts say, is the small market share Apple has, particularly in the enterprise. However, that is gradually changing and the attackers are beginning to follow.

In addition to the new crimeware kit, a Mac-specific scareware attack also popped up on Monday, targeting users who searched for some popular terms on Google. The MACDefender scareware is appearing in search results for images of Osama bin Laden as well as in other places.

"In it's current incarnation, MACDefender shows up in the installed applications list, so can be uninstalled. If you have accidentally installed this, go ahead and uninstall it. I would not expect this 'uninstall' option to be a good long term protection strategy. I'd suggest that OSX users disable 'Open safe files after downloading', and also invest in a reasonable anti-malware suite. Installing a real anti-malware package is also a good idea," Rob VandenBrink of the SANS Internet Storm Center wrote in an analysis of the scareware.

Apple Laptop Batteries Can Be Bricked, Firmware Hacked

By Dennis Fisher

Security researcher Charlie Miller, widely known for his work on Mac OS X and Apple's iOS, has discovered an interesting method that enables him to completely disable the batteries on Apple laptops, making them permanently unusable, and perform a number of other unintended actions. The method, which involves accessing and sending instructions to the chip housed on smart batteries could also be used for more malicious purposes down the road.

The basis of Miller's research, which he plans to present at the Black Hat conference in Las Vegas next month, is the battery that's used in most Apple laptops. The battery, like many others in modern laptops, has a chip on it that contains instructions for how the battery is meant to behave and interact with the operating system and other components. Inspired by Barnaby Jack's ATM hacking talk at last year's conference, Miller was interested in seeing what would happen if he could get access to the chip and start messing with the instruction set and firmware.

A lot, as it turns out.

"The battery has its own processor and firmware and I wanted to get into the chip and change things and see what problems would arise," said Miller, a principal research consultant at Accuvant.

What he found is that the batteries are shipped from the factory in a state called "sealed mode" and that there's a four-byte password that's required to change that. By analyzing a couple of updates that Apple had sent to fix problems in the batteries in the past, Miller found that password and was able to put the battery into "unsealed mode."

From there, he could make a few small changes to the firmware, but not what he really wanted. So he poked around a bit more and found that a second password was required to move the battery into full access mode, which gave him the ability to make any changes he wished. That password is a default set at the factory and it's not changed on laptops before they're shipped. Once he had that, Miller found he could do a lot of interesting things with the battery.

"That lets you access it at the same level as the factory can," he said. "You can read all the firmware, make changes to the code, do whatever you want. And those code changes will survive a reinstall of the OS, so you could imagine writing malware that could hide on the chip on the battery. You'd need a vulnerability in the OS or something that the battery could then attack, though."

In his lab, Miller was able to brick the battery so that it wouldn't take a charge or discharge any power, and he said it's also possible to send faulty instructions to the OS, giving it bad information about the level of power left in the battery. He wasn't able to accomplish his main goal, however.

"I started out thinking I wanted to see if a bad guy could make your laptop blow up. But that didn't happen," he said. "There are all kinds of things engineers build into these batteries to make them safe, and this is just one of them. I don't know if you could really melt the thing down."

Miller plans to release a tool at Black Hat that will go in and change the default passwords on the battery's processor so that the hacks he developed won't work. It will lock the battery in sealed mode permanently.

What About Fob?

Few things sent shockwaves to all corners of the security community like news in March that RSA's popular SecurID two-factor authentication tokens had been rendered all but useless by a small but cleverly targeted phishing campaign that included a payload of a malicious Flash object embedded in an Excel file. Once inside RSA's networks, the hackers feasted on SecurID user data from corporate customers and other organizations that used the tokens to grant access to corporate networks, e-mail and other sensitive assets. Despite assurances that SecurID's effectiveness had only been marginally compromised, RSA was forced to recall 40 million of the tokens in June.

RSA: SecurID Attack Was Phishing Via an Excel Spreadsheet

By Dennis Fisher

RSA confirmed on Friday that the attack that compromised the company's high-value SecurID product was essentially a small, targeted phishing campaign that included a payload of a malicious Flash object embedded in an Excel file.

The much-discussed attack on RSA, which the company revealed last month, resulted in the company warning customers that the security of their SecurID authentication tokens may be reduced. Speculation about the exact nature of the attack has been rampant in the security community ever since the disclosure, and RSA has been quite tight-lipped about the details of the incident.

But on Friday the company briefed analysts about the details of the attack and then published a series of explanatory blog posts that spilled some, but not all, of the specifics about the incident.

"The attacker in this case sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read '2011 Recruitment Plan," Uri Rivner, head of new technologies in the identity protection division of RSA wrote in a post on the attack.

"The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled '2011 Recruitment plan.xls.'

The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609)."

An RSA spokesman confirmed that the blog posts and attack details were authentic.

What Rivner described--and what RSA apparently detailed for industry analysts--is the textbook definition of a targeted phishing attack. What the attacker goes after and obtains once inside the compromised network largely depends on which user he was able to fool and what that victim's access rights and position in the organization are.

The malware that the attacker installed was a variant of the well-known Poison Ivy remote administration tool, which then connected to a remote machine. Rivner, as well as other RSA employees in their own posts, discussed the attack as an example of an APT (advanced persistent threat), although the method was essentially a spear phishing attack. The emails were sent to what Rivner said was a small group of RSA employees, at least one of whom pulled the message out of a spam folder, opened it and then opened the malicious attachment.

"Having set remote access, now the attacker in a typical APT starts digital shoulder surfing to establish the employee's role and their level of access. If this isn't sufficient for the attackers' purpose, they will seek user accounts with better, more relevant, privileges," Rivner said.

"When it comes to APTs it is not about how good you are once inside, but that you use a totally new approach for entering the organization. You don't bother to just simply hack the organization and its infrastructure; you focus much more of your attention on hacking the employees."

The description of the attacker's tactics once inside RSA's network is quite similar to what security researchers say are common techniques used to obtain, package up and exfiltrate sensitive data.

"The attacker first harvested access credentials from the compromised users (user, domain admin, and service accounts). They performed privilege escalation on non-administrative users in the targeted systems, and then moved on to gain access to key high value targets, which included process experts and IT and Non-IT specific server administrators," Rivner said in his description of the attack.

"The attacker in the RSA case established access to staging servers at key aggregation points; this was done to get ready for extraction. Then they went into the servers of interest, removed data and moved it to internal staging servers where the data was aggregated, compressed and encrypted for extraction. The attacker then used FTP to transfer many password protected RAR files from the RSA file server to an outside staging server at an external, compromised machine at a hosting provider. The files were subsequently pulled by the attacker and removed from the external compromised host to remove any traces of the attack."

Mobile Madness

Admit it. It would scarcely break your heart if the legions of slack-jawed smartphone Facebook and FourSquare gawkers were forced to confront their own digital mortality – however briefly -- with a few scary exploits made just for them. In 2011, the untethered among us saw several mobile security challenges to be concerned about. High on the mobile hackers' hit list is Android, the market-leading smartphone OS. Among the highest profile malware was a new variant of Android Trojan called ANDROIDOS_NICKISPY.C that masquerades as a Google+ app and has the ability to intercept record phone calls, but also to answer incoming calls and respond to remote commands sent via SMS. Worse yet, Google was twice forced to delete dozens of apps from its Android Market after the programs were found to be infected with DroidDream, malware that captures and transmits phone user data to a remote server for malicious purposes not yet fully known.

Android Malware Found Stealing Texts, Intercepting Calls

By Dennis Fisher

The steady drumbeat of malware and spyware targeting the Android platform is continuing, this time with

the emergence of a new variant of an Android Trojan that masquerades as a Google+ app and has the ability to not only record phone calls, but also to answer incoming calls and respond to remote commands that arrive via SMS.

The new piece of malware is known as ANDROIDOS_NICKISPY.C and has some powerful functionality. The most interesting feature the malicious app sports is its ability to intercept incoming calls and prevent the user of the infected device from even knowing that the call came in. Also, according to researchers at Trend Micro, ANDROIDOS_NICKISPY.C has a predefined controller number that, when attached to incoming SMS messages, can be used to issue commands to the infected device.

And, if a phone call comes from that controller number, the malware has the ability to intercept it, silence the device so the user isn't aware of the call and hide the keypad from the user.

"Like other ANDROIDOS_NICKISPY variants, ANDROIDOS_NICKISPY.C also has the capability to record phone calls made from infected devices. What makes this particular variant different is that it has the capability to automatically answer incoming calls," Mark Balanza, a threats analyst at Trend Micro wrote in an analysis of the malware.

"Before answering the call, it puts the phone on silent mode to prevent the affected user from hearing it. It also hides the dial pad and sets the current screen to display the home page. During testing, after the malware answered the phone, the screen went blank."

Balanza said that the malware only has the ability to intercept incoming calls on Android devices that are running version 2.2 or earlier of the operating system. Like earlier versions of the malware,

ANDROIDOS_NICKISPY.C has the ability to gather GPS location, text messages and call logs and send them off to a remote machine. ANDROIDOS_NICKISPY.C installs on infected devices with a copy of the Google+ icon, but the app shows up as Google++.

Android has become a frequent target for attackers in the last few months as the popularity of the platform has continued to grow. There have been cases this year of SMS Trojans being found in Android apps in the Google Market, dozens of apps infected with the DroidDream malware showing up in the Market and a number of other incidents. The iPhone has been a less frequent target for malware authors, relatively speaking, than Android devices have, perhaps as a result of Google's more open policy with the Android Market and the platform in general.

DroidDream Returns, Dozens of Apps Pulled From Android Market

By Dennis Fisher

Researchers have identified a second large batch of apps in the Android Market that have been infected with the DroidDream malware, estimating that upwards of 30,000 users have downloaded at least one of the more than 30 infected apps. Google has removed the apps from the market.

There are at least 34 applications that researchers have found in the Android Market in the last few days that had a version of the DroidDream malware dropped into them. Once a user installs one of the infected applications, the malicious component, which researchers have dubbed DroidDream Light, will kick in once the user receives an incoming call. The malware then gathers some identifying information from the phone, including its IMEI number, IMSI number, packages installed and other data, and then sends it off to a pre-configured remote server.

There are apparently six developers whose apps have been infected with DroidDream Light in the last few days.

"Malicious components of DroidDream Light are invoked on receipt of a android.intent.action.PHONE_STATE intent (e.g. an incoming voice call). DroidDream Light is not, therefore, dependent on manual launch of the installed application to trigger its behavior. The broadcast receiver immediately launches the <package>.lightdd.CoreService which contacts remote servers and supplies the IMEI, IMSI, Model, SDK Version

and information about installed packages. It appears that the DDLight is also capable of downloading and prompting installation of new packages, though unlike its predecessors it is not capable of doing so without user intervention," researchers at Lookout Mobile Security wrote in an analysis of the new version of the malware.

The list of infected apps includes:

- Floating Image Free
- System Monitor
- Super StopWatch and Timer
- System Info Manager
- Call End Vibrate
- Quick Photo Grid
- Delete Contacts
- Quick Uninstaller
- Contact Master
- Brightness Settings
- Volume Manager
- Super Photo Enhance
- Super Color Flashlight
- Paint Master
- Quick Cleaner
- Super App Manager
- Quick SMS Backup
- Tetris
- Bubble Buster Free
- Quick History Eraser
- Super Compass and Leveler
- Go FallDown !
- Solitaire Free
- Scientific Calculator
- TenDrip

This is the second major incident involving DroidDream-infected apps in the Android Market. In March, Google pulled another large batch of infected apps from the market and later remotely removed from the devices of users who had downloaded them. It's not clear whether Google will use that capability again, but the company has not been shy about doing so in the past when malicious apps have been identified in the Android Market.

Not Again! Duqu Hits Iran

Pity poor Iran. They can't catch a break. After cleaning up the mess Stuxnet wreaked on their nuclear ambitions, the Middle Eastern country admitted in November that a number of machines across multiple industries were infected with Duqu. While academic arguments raged over whether similarities in source code proved Duqu was the spawn of Stuxnet, researchers digging around under the worm's hood discovered some interesting and unique characteristics. Where Stuxnet was designed to damage SCADA-driven industrial machines, Duqu seems more intent on monitoring user activity and stealing data. And Duqu is delivered via an infected Microsoft Word file attached to a highly customized and targeted phishing email. As the year winds down, Iranian officials say they've distributed software to rid computers of the Duqu menace. But it's likely the entire impact of Duqu infections remains unknown and, will only fully reveal itself later in 2012.

Such is the way a new list begins. Happy New Year!

Duqu Attackers Using Word Docs As Attack Vector

By Dennis Fisher

As the analysis of the Duqu malware continues to evolve, the picture that's emerging is becoming more and more intriguing. The latest bits of evidence uncovered show that not only do the attackers create custom files for each individual attack, there is evidence indicating that they might have been working on Duqu in some form since 2007.

The newest analysis of the malware found that there are some drivers associated with the Duqu files that

are dated as far back as 2007. Another driver found during the investigation has a date of 2008. The analysis is based on a couple of specific Duqu infections, and coupled with the files and drivers that have been discovered previously, researchers say that it now looks certain that whoever is behind Duqu is tailoring each attack specifically to each new target, right down to creating new files for the attacks on the day that they're performed.

Duqu infections are multi-stage operations, but they begin much like many others: with a targeted phishing email. In the cases analyzed by researchers at Kaspersky Lab, the email contains a Word file that includes the exploit code. Once a victim opens the file, the exploit fires in the background and begins the installation process. The malware becomes resident in the machine's memory, but it doesn't actually do anything for a few minutes, until the user goes idle. When that happens, the shellcode, which is contained in an embedded font called Dexter Regular, starts its work.

"The driver loaded by the exploit into the kernel of the system had a compilation date of August 31, 2007. The analogous driver found in the dropper from CrySyS was dated February 21, 2008. If this information is correct, then the authors of Duqu must have been working on this project for over four years," Kaspersky chief malware expert Aleks Gostev wrote in his analysis.

The analysis is based on what is believed to be the first known Duqu infection, the attack in Iran earlier this year that Iranian officials said was the result of a piece of malware they called Stars. It now appears that Stars was in fact an earlier version of Duqu, Gostev said in his analysis.

"Most probably, the Iranians found a keylogger module that had been loaded onto a system and which contained a photo of the NGC 6745 galaxy. This could explain the title Stars given to it. It's possible that the Iranian specialists found just the keylogger, while the main Duqu module and the dropper (including the documents that contained the then-unknown vulnerability) may have gone undetected," he wrote.

The shellcode used by Duqu changes with each new target, as does the Word file that's included in the attack email. Each one is tailored to the individual target. And, it looks as if each new attack uses a separate command and control server. At least one of the known C&C servers, which was located in India, has been taken offline. The location of the newest control server isn't being made public at this point, but Gostev said that it appears that it may not be working at this point.

About Threatpost

Threatpost, Kaspersky Lab's Security News Service, is dedicated to helping IT security professionals succeed by delivering the most important and immediate security news and analysis available. Threatpost off ers a fresh approach to providing up-to-the minute news and information for IT security and networking professionals. Threatpost editors cover today's most relevant security news and the most pressing security issues of the day. They break important original stories, off er expert commentary on high-priority news aggregated from other sources, and engage with readers to discuss how and why these events matter. Threatpost's global editorial activities are driven by industry-leading security journalists Dennis Fisher and Paul Roberts. They are assisted by Ryan Naraine, a widely-followed security journalist and regular contributor to Threatpost.

Collectively they bring over thirty years of experience to their mission of delivering insight into the issues that aff ect the lives of security professionals every day. Threatpost has expanded with Latin American editions in both Spanish and Portuguese. These editions are led by local, veteran editorial teams dedicated to covering security news and analysis vital to the region.

Make Threatpost your first stop for security news and analysis.
www.threatpost.com