acmqueue

CTO Roundtable: Malware Defense

The battle is bigger than most of us realize.

As all manner of information assets migrate online, malware has kept on track to become a huge source of individual threats. In a continuously evolving game of cat and mouse, as security professionals close off points of access, attackers develop more sophisticated attacks. Today profit models from malware are comparable to any seen in the legitimate world.

But there's hope. Some studies have shown that while 25 percent of consumer-facing PCs are infected by some sort of malware, the infection rate of the commercial PC sector is around half that rate. This difference is most likely a direct result of the efforts of security professionals working in commercial sites to defend against these threats.

Today's CTO Roundtable panel is our fourth and is split between users and vendors. During the course of our conversation on malware defense, we plan to educate readers about the scope of the malware threat today, the types of frameworks needed to address it, and how to minimize the overall risk of breach.

Leveraging the academic roots and vendor-neutral focus of ACM, CTO Roundtables help define and articulate general best-practices consensus on newly emerging commercial technologies. Through our panels, we provide practitioners with valuable access to objective and unbiased expert advice on what folks should and should not focus on in the next one to three years. —*Mache Creeger*

PARTICIPANTS

MICHAEL BARRETT is the CISO (chief information security officer) of PayPal.

JEFF GREEN is head of the threat research unit at McAfee Lab, where his role has been unifying the siloed research around e-mail, Web site, spam, phishing, and malware to support businesses around remediation management, patch management, risk, and compliance.

VLAD GORELIK is vice president of engineering at AVG Technologies. He is responsible for what AVG calls behavioral chronologies—nonsignature malware defenses. He has been working on nontraditional malware defenses for the past six or seven years.

VINCENT WEAFER is vice president for security response at Symantec. His group focuses on malware defense, handling phishing, frauds, threat intelligence, URL data feeds, and reputation.

OPINDER BAWA is the CIO for the University of California, San Francisco (UCSF) School of Medicine.

STEVE BOURNE is CTO at El Dorado Ventures, where he helps assess venture-capital investment opportunities. Prior to El Dorado, Bourne worked in software engineering management at Cisco, Sun, DEC, and Silicon Graphics. He is a past president of ACM and chairs both the ACM Professions Board and the ACM *Queue* editorial board.

MACHE CREEGER is the moderator for the CTO Roundtable series. He is the principal of Emergent Technology Associates, providing marketing and business-development consulting services to technology companies focused on enterprise infrastructure.

CREEGER Let's start off the discussion by providing an assessment of the malware threat as you see it today.

WEAFER The past 12 months in the malware-threat landscape have been a natural evolution of the past couple of years. We have seen a huge explosion in the volume of new malware. We've also seen evolution in terms of the sophistication of malware, new data-mining techniques, and new methods of self protection that have really changed the threat landscape. The attacker's ability to get smarter tools easily and use them faster with less technical skill has changed a lot of what we're seeing.

We are not looking at a single pandemic threat but a huge explosion of individual threats. What you get on one machine is completely different from what you get on another machine. Each infection has a unique signature. You're served up a unique piece of malware that may not be seen by anyone else in the world. Threats have gone from global to local to personalized.

GORELIK I agree. You are also seeing automated tools for distributing malware: for finding sites that are vulnerable, attacking them, and turning them into distribution sites. Once you start automating, it becomes a much broader distribution model. You start seeing ways to reach many more people in one shot and more innovative profit models and social engineering techniques. These models are fairly sophisticated and on par with marketing seen in the legitimate world.

BARRETT About four years ago, when I was at American Express, I asked the question, how many desktop PCs on the Internet have been compromised? It was surprisingly hard to get an answer, as industry does not seem to track that issue. About a year ago, I succeeded when I talked to some folks at Georgia Tech. Based on their research, they believed the number was almost exactly 12 percent.

What's interesting about this is if you talk to consumer-facing ISPs, the numbers are more in the 25 percent range. The difference between the total number and the consumer-facing segment suggests that field-security practitioners working in the nonconsumer sector are actually having an impact.

BAWA A lot of malware that we see is twofold. We see general malware, things on our computers that are trying to capture information such as a Social Security number and send it to some collection point. These are more generic, general attacks at a possibly superficial level. We also find a lot of very specific, custom software components that will say, "If they exist, go through these databases, scan for this information, and send me these 2 million transactions."

In the medical industry we see a complete set of problems—from downloading movies to targeting databases for Social Security numbers, and the latest trend, which is stealing medical information.

If someone stole 100 Social Security numbers, that person could sell them on the street for around $3 to $4 each. If someone steals a person's medical information, the thief can sell it for thousands of dollars to someone in the United States who needs to see a doctor to get an operation.

GORELIK This demonstrates that malware is a business. At the end of the day, these guys are there to make money. If they see high-margin information they can steal for leverage, they're going to go after it. As the market gets saturated by things such as Social Security numbers and credit card numbers, their values drop, so people move to higher-value targets.

WEAFER If I can combine your physical address with your financial information or e-mail address, it's more valuable to the attackers. Refining content from low-value information that is raw and without context to high-value specialized content is definitely a growing trend.

While we as vendors are seeing an increase in both sophistication and volume, paradoxically user awareness is dropping. Apart from Conficker, which has gotten a lot of attention over the past few months, the opposite has occurred over the past few years. The perception is that the malware and

spyware problems of the early 2000s have gone away and things are safer. You are seeing people with less awareness and with the perception that they don't need to worry. The challenge is how, in a nonalarmist way, to keep people aware of the dangers.

BARRETT There is good data suggesting that a lot of people think their PCs are protected when they are not. They either mistakenly assume that because a PC came with a preinstalled AV (antivirus) product, its protection lasts a lifetime, or worse, they think they have paid for a subscription to update it and have not. That turns out to be quite a systemic problem.

GORELIK In fact, it is even nastier. We are seeing quite a bit of fake antivirus protection being pushed out. It looks real and sometimes even has a small AV engine with a small set of signatures. In reality though, it's also infecting the host machine.

BAWA Older institutions have machines that run Windows 2000, Windows 95, and Windows 98. They are typically in laboratories connected to specialized equipment and are not easily upgraded. Generally, there is a low awareness of the implications of that vulnerability.

CREEGER What can people do to avoid these threats?

BAWA SCO (Santa Cruz Operation) focused on the SMB (small to medium business) market. SMBs with fewer than about 50 employees usually have an IT provider that they trust—not a national chain but just a local mom-and-pop shop. At more than 50 employees, companies hire a system administrator/IT manager/IT person. That person usually tries his or her best, but has a very difficult task keeping everything running and updated and often is not effective.

The segment between 50 and about 250 employees is not being well served. Companies with fewer than 50 or more than 250 employees have viable options, but inside that range, companies have very limited options for effective IT support.

GREEN We just did a broad survey of small to medium companies. The results clearly stated that in this segment, the average IT administrator spends less than one hour a month on security.

CREEGER Aren't people afraid? Since folks don't see the direct results of poor security in their face all the time, is malware more of an insidious type of threat today?

WEAFER With the silent nature of these current attacks, many people are obviously unaware of the risk or damage to their personal data. Moreover, there are many more who just don't care. They can still open their documents, still effectively work, so they choose not to worry. There is certainly a lack of awareness with regard to some of the newer attack techniques. There's the perception that what I don't see won't hurt me.

CREEGER You're saying that malware writers are getting more sophisticated. They've learned that if they minimize the direct impact to the computing platform so that the effects of their attacks are not "in your face," then they can get much more value from those machines.

WEAFER Absolutely. I call it slow and low. If you attack a machine slowly and silently, you'll extract maximum profit over a longer period of time than doing something aggressively, being seen, and then being stopped quickly.

BARRETT At PayPal we have concluded that it isn't just malware that is the problem; the average Internet consumer has had no training on what represents safe behavior. We have to get out and help teach them that. We have concluded that putting words on Web pages is a fairly poor educational medium. We try to simplify our customer safety messages and take them to where consumers hang out.

CREEGER When I talk to other experts, they say it goes way beyond that. If you visit questionable

Web sites, shady areas of less than ethical intent—such as pornography or pirated software (warez) sites—you don't have to execute object code from some random e-mail or visit a Web site from a link provided by some phishing e-mail. The fact that you've just visited the site is enough to get an infection.

BARRETT That may be true if you have not kept your PC patched. In our set of messages around PC safety, we say three things:

- Run a modern operating system. If you use Windows 95 to surf the Internet and visit one of those Web sites, you have a very good chance of being compromised.
- Keep those updates turned on. Not being up to date on operating-system patches was the mistake made by all the Conficker victims.
- Also run an up-to-date antivirus program with the latest security updates.

Do those three things and you substantially lower your risk of infection. Are you 100 percent safe? No, but you're not 100 percent safe crossing the street either.

BAWA I have a different perspective. There are some things users can be taught and there will be a real change. Generally speaking, security is not one of them. If we're counting on users to do the right thing at all times, it's never going to happen. Very simply, users expect that the operating system and the environment are secure and that they are protected by antivirus software that comes with malware protection. They believe that protection is what they purchased and if it's not doing the job, they are not getting what they paid for.

BARRETT I'm sympathetic to your point of view, but would say that societies can choose what represents safe and unsafe behavior and can legislate against deliberately unsafe behavior. As a society, we believe that it is important to drive safely on the road. If you go flying down a busy city street at excessive speed and kill somebody, you will probably go to jail for vehicular homicide.

There are no intrinsic reasons why we can't impose limits on unsafe behavior that actually jeopardizes others on the Internet. The most insidious thing about malware is that it isn't a threat just to you; it is also a threat to Internet safety at large.

GORELIK One of the issues with your analogy is that driving down a crowded city street at high speed has direct and immediate consequences. Malware does not work that way. If you do get infected, and even if you clean it up, you might not see the direct consequences of that infection or be able to tie that infection to consequences suffered by someone else.

It is very difficult for a user to make that connection. The impact of malware infection is disconnected compared with something much more physical and tangible. I agree that education would help, but there are limits to its effectiveness.

BARRETT Too many people find out how to protect themselves on the Internet through ad hoc means such as talking to people at cocktail parties. They may find out things such as avoiding phishing scams by looking out for poorly spelled e-mails and Web sites without any graphics. Often that advice may have been true years ago but is no longer valid today.

Recently we were told by one of our security providers that a number of our customers had shown up on a Sinowal trojan drop server list (http://news.bbc.co.uk/2/hi/technology/7701227.stm). We had a big file of these and we are notifying those customers saying the following:

- We're terribly sorry, we believe your PC has been compromised because these are your details and they match all the data we store on you.
- This is how you probably got infected.

- Go here for advice on how to fix your PC.
- By the way, some malware is so nasty you're going to have to clear the machine and rebuild it from base hardware or take it to somebody who actually can rewrite the master boot record.
- Here's a PayPal security key to help protect you.

It's a whole get-well kit. I think we're probably one of the first companies to attempt this. As an industry we are going to have to do more of this kind of outreach.

CREEGER Is that possible today given the architecture of existing operating systems? I have been told that there's some really nasty stuff out there and if you poke it the wrong way it will crash the machine.

WEAFER The vast majority of stuff does not require that kind of drastic action. While there's absolutely some really bad malware out there, there is still an enormous amount of fairly basic stuff that can be taken care of without a bare-metal rebuild.

One thing that's increasingly happening is that Web sites, particularly those owned by small businesses, are being compromised. These sites are in turn being used to attack others. So it's not just the problem of the desktop owner, but now the Web-site owner as well. Among the biggest infection vectors we see today are threats being delivered onto user systems from compromised Web sites. If you are an owner of a Web site, you need to pay attention to this problem. This is really challenging for small business because most of those people have no idea what Web-site security really entails.

Some hosting companies will do security scans as part of their service, or you can go to specialist boutiques or service providers. Depending on the type of infection, however, malware removal by this means could be very difficult.

CREEGER It sounds like a small to medium business has to understand a lot of detail in order to address the risks we have been talking about. Are there people who can take over that function? For small to medium business owners responsible for the company's Web sites and PCs, what should they do and what are the tradeoffs? What should they be thinking about? How big does an organization have to be before it hires an in-house expert?

BAWA We do a risk-to-reward security analysis for any potential insecurity we come across. This helps determine the cost benefit for any given solution to ensure we're focused on the highest risks at all times.

Consumers expect to buy one product that does everything. In the small to medium business market, companies start to understand that if they are setting up Web sites, they are going to need some protection, but they don't know what that is. They turn to their small IT provider to provide that package. When you get to a $100 million company, you are going to be concerned about DLP (data loss prevention). If you're a $5 million company, you're not, because you know everybody and it's much more of a trusting environment.

BARRETT One of the most basic defenses is have good practices around patching. If you have an endpoint, keep it patched, and run up-to-date AV, then that goes a long way toward providing reasonable protection.

BAWA People also want value. Once they understand they need these five different components for protection, they look for value. The one common question that all SMBs will ask is, "What product can I buy that gives me the most features for the best price?"

CREEGER Trying to figure out what the value is for the money spent is a bit of a gamble. People naturally don't want to spend a lot of money, but they don't have any effective way of evaluating what their exposure is, given a particular level of spending.

GREEN There isn't a strong enough appreciation for the volume and propensity of malware that we're dealing with. When you tell people the number of threats we see per day, their jaws just drop to the table.

WEAFER It's the dynamic nature of malware attackers that if you defend against something, things will change. Security is very different from the more stable and predictable areas of computing such as storage and search. When one hole is plugged, attackers simply move on to attack different areas.

CREEGER You are telling me that you have a highly adaptable adversary and that it is very difficult to assess risk and asset value. You're trying to plug as many leaks as you can with a fixed budget, and there's no real guarantee that what you left out wasn't the critical thing that will sink your boat. Is there any good news here?

WEAFER The good news is that people who take the basic commonsense actions seem to be less impacted on a consistent basis. This is the good hygiene story where the guy who just washes his hands before meals seems to get sick far less often. Even though new technology and new trends are being seen all the time, the basic best practices haven't changed all that much.

GORELIK There are two kinds of attack models. One is to cast a wide net and pull in whatever you catch. As a user, if you do the basic commonsense things, you're probably reasonably protected. There are also guys who are going to target you because you have something of value. Security here should be more sophisticated and based on the impact of a successful breach.

BARRETT This attack is based in the attacker's perceived value of the assets you have on your system and brings to mind the old joke about what to do if you are attacked by a bear in the wilderness. The answer is that you don't have to outrun the bear, you just have to outrun the guy next to you. To the extent that attackers perceive that you have juicy assets, but you seem to have done a half-decent job of locking things up, attackers may go try the bozo next door who has probably done a less competent job.

BOURNE From a defensive perspective, are there things people were doing last year that have stopped working?

WEAFER Up to recently we would say that if you avoided going down the dark alleys of the Internet—the pornography sites, for example—you were probably safe. Because of the rise of cross-site scripting attacks that inject malicious code into otherwise normal Web pages, that is not so true anymore.

GORELIK You now have to be careful of legitimate software that has been repackaged to include other executables containing threats. Also, in the past people could safely download software that was not signed. At this point, I would not download anything that's not signed—and signed by an entity I trust. You have no way of guaranteeing that the integrity of the software has not been tampered with on the server.

I did an experiment and went to a reasonably well-known site and downloaded a whole bunch of stuff. When I first started seeing a large number of compromised executables, I thought that the problem was in our testing process. Sadly, it turned out that our process was just fine, but the files had really been infected.

BAWA But it's not just about trusting. In October 2008 people visiting the Macys.com retail site got hijacked to a Web site that looked like Macys.com but wasn't.

BARRETT I believe owners of consumer-facing Web sites have a responsibility not only to ensure that their infrastructure is secure, but also to demonstrate that theirs is a legitimate Web site. We pay a nontrivial uplift to have extended validation. When you go to PayPal.com with a modern operating system and browser, you get a green glow object in the address bar that says, PayPal, Inc.—not in the URL itself but beside it. These are the kinds of definitive user interface cues that consumers can and should be looking for.

WEAFER I believe we will see more reputation-based security models. Black-and-white listing-based protection is a simpler version of this. You're seeing examples of reputation protection in browsers offering warnings about unsafe sites with file downloads showing whether the files were signed or from a trusted sources and whether e-mail senders are on a known spam list. These are all examples of simple reputation-based security and imply a trend toward a more general model that provides the user with a full reputation on what they download or use. The user's appetite for risk then determines whether the transaction proceeds.

CREEGER Could cloud computing help or hurt these types of issues? What does cloud computing do for these types of vulnerabilities? If people start moving their services out onto cloud platforms, are they better or worse off?

BARRETT Cloud computing is very promising for cost-effective and burst capacity. There is a very large user base of organizations that are attracted to cloud computing where they deal with nonconfidential information. There are also people who represent more regulated industries, such as financial, that cannot just dump the data in an outsourced cloud and not know its physical location. I have to know where my data resides because there are safe-harbor considerations I must maintain. So the data-location requirement is one issue with clouds.

A second issue is the ability to define an application's security requirements. If I have particular security requirements around my application, I don't want it to co-reside with someone else's application that has a different requirement set. We don't have the policy language yet to adequately describe everyone's security requirements. For cloud computing to work, that type of definitional information needs to be in place. It is not there today, but we will undoubtedly get to the point where we will have the proper risk vocabulary to address this issue.

Most of the cloud vendors at this point are using comparatively basic security patches that are perfectly functional, and as I said earlier, a little patching goes a long way. They are demonstrating to prospective clients their SAS70 (http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations), and you can review it to determine whether their controls are adequate.

CREEGER What are the more interesting and surprising types of malware you have experienced?

BARRETT ATM malware targets a specific vendor's ATMs. The bad guy wanders up to the ATM, opens up its externally accessible maintenance port, shoves in a USB stick, and takes it over. The victim happily uses the ATM while it does things the bank doesn't know and didn't intend. This is not at all common as yet and occurred only because somebody was able to steal the source code for that particular ATM.

BAWA A service person came in and put malware on the point-of-sale devices for six or eight local San Francisco Bay area gas stations and captured all the debit cards.

BARRETT For various reasons, debit cards are often more attractive targets than credit cards.
CREEGER On the malware defense side, what surprisingly innovative things have vendors produced in the past few years?
WEAFER Reputation-based security is very interesting—cloud-based plus reputation-based. Reputation is a good way to deal with environments that are not heavily regulated and not able to be locked down.
BARRETT One of the most interesting trends in the past year or so is the active research community letting machines get infected by bits of malware. They are trying to work out what the malware is being used for, how it's engineered, and what greater purpose it serves. The best example is the folks who took apart the Storm network and determined that its purpose was to spam Viagra ads. They really understood the mechanics of how that particular botnet was put together.
WEAFER There's a lot more ongoing research evaluating the ecosystem and looking at every part of the crime life cycle—not just the technology pieces but who benefits from the crimes. Who is making money, how are they doing it, where is it happening, and how are they controlling it? Ultimately, we are looking for effective levers to combat malware. Sometimes these levers may be technology based, sometimes policy based.
BARRETT Malware isn't fundamentally a technical problem; it's a crime problem. Even though we and other financial services firms have seen a lot of consumers have their credentials stolen, the average level of victimization is usually very low. The criminal market has so many credentials available at this point that the bottleneck is not in acquiring more credentials, it's in monetizing them.
CREEGER Can ISPs provide effective malware defense?
WEAFER ISPs need to engage their users and provide not only technology help but also policy help around this problem. The ISP is for many people the closest thing they have to a touch point on the Internet. When a user infection is identified, the ISP should engage the user in a positive dialogue and work to resolve the problem for the good of the entire community. Letting the problem fester or moving it to another vendor should not be a viable alternative.
BARRETT The force at play is what economists call *negative externalities*. Decisions are made by one party, but the costs are borne by others. The costs resulting from users browsing dubious Web sites on unprotected machines and getting infected are borne not just by the ISP but by the Web sites that may get attacked from the infected user. That user's browsing behavior has real and measurable costs to those businesses. The argument here is simply, what is the set of economic and regulatory policies that will influence users to better align their decisions with its cost impact on the rest of the community?
CREEGER It's the same argument as public health.
BAWA I have a very different opinion on this. Living in the technology world, you become analytical: How do I fix? What are the data points? and so on. I think security and some of the issues we're facing are more like influenza, where every year there's going to be another strain no matter what you do. You can do everything right and there will still be another strain. Technology and policy have solved certain things very well: CRM (customer relationship management) systems, supply chain, iTunes… Security is an environment that is ever changing, and unless we understand that, we're going to be chasing our tail for a long time.
CREEGER I want to thank everyone for sharing your experiences and perspectives. It is clear to

me that malware defense is an evolving area that is extremely dynamic and has equal measures of both art and science. This discussion has given our audience a better understanding of the threat landscape and an appreciation for what they should be thinking about to reduce the risk of compromise. Hopefully it will encourage folks to evaluate their security architectures to be more in tune with the risks they face. Q

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org