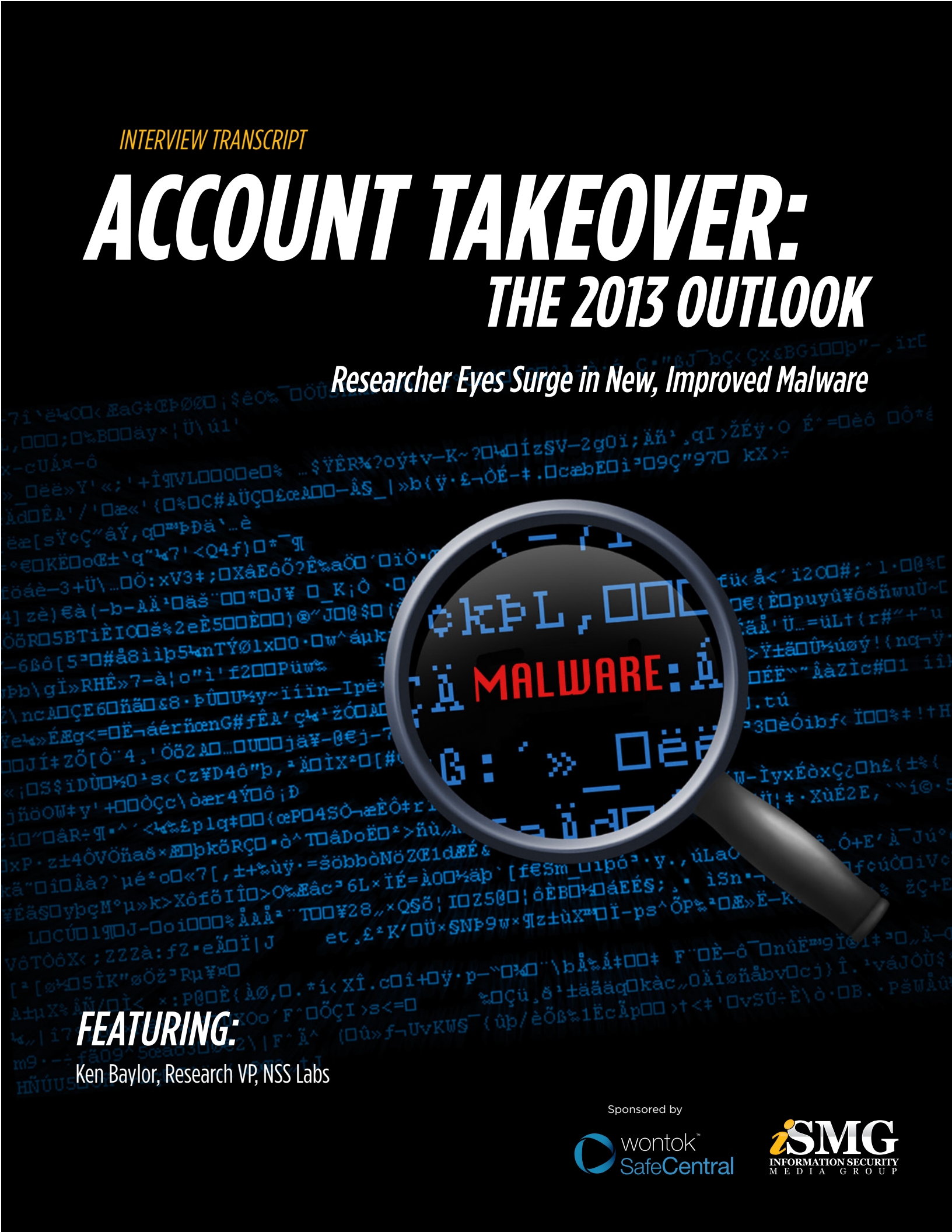
INTERVIEW TRANSCRIPT

ACCOUNT TAKEOVER: THE 2013 OUTLOOK

Researcher Eyes Surge in New, Improved Malware



FEATURING:

Ken Baylor, Research VP, NSS Labs

Sponsored by

wontok SafeCentral

iSMG INFORMATION SECURITY MEDIA GROUP

wontok SafeCentral

iSMG INFORMATION SECURITY MEDIA GROUP

It has been nearly four years since the advent of the current account takeover schemes that see banking institutions and their customers victimized by ACH/ wire fraud.

And it has been almost two years since the release of the FFIEC authentication guidance supplement, aimed in part at helping institutions detect and prevent takeover attempts.

So, as 2013 begins, what is the state of account takeover?

Read on to hear from a security research expert:

- The current account takeover trends;
- The latest malware variants;
- Effective strategies and solutions for fighting takeover fraud.

Ken Baylor
Research VP, NSS Labs

Baylor currently serves as research VP at NSS Labs. Recently he was the vice president of antifraud strategy and emerging threats at Wells Fargo. He is widely recognized as a leader in bank security, IT security and regulatory compliance and as a speaker at leading industry events such as RSA, BlackHat, Bloomberg Enterprise Risk and FS-ISAC. He previously served as CISO at Nuance, as Vice President of IT and Chief Information Security Officer (CISO) at Symantec, and is a Certified Information Systems Security Professional and a Certified Information Systems Manager.

"This is a cat-and-mouse game where we're constantly, slowly escalating."

TOM FIELD: To start out, please tell us a little bit about yourself and your own banking and security experience.

KEN BAYLOR: I currently serve with NSS Labs as the research VP. Previously, I was vice president of anti-fraud strategy and emerging threats over at Wells Fargo. Before that, I served as a chief information security officer at Nuance and also at Symantec. Primarily, I focus on bank security, IT security and regulatory compliance. I regularly speak at industry events like RSA, BlackHat, Bloomberg Enterprise Risk and FS-ISAC.

State of Account Takeover

FIELD: The industry has been talking about account takeover pretty steadily for nearly four years now. Give us a baseline. What do you see as the state of account takeover today, what type of malware are we seeing and what damage do you see it doing?

BAYLOR: We're still seeing Zeus and its various forms leading the pack. Zeus is by far the best platform for stealing money from banks, and it compromises multi-factor authentication very easily. It's caused hundreds of millions of dollars in bank losses worldwide. With the leak of the Zeus 2.0 source code in summer 2011, we've seen a major proliferation of malware stemming from this stolen source code. A lot of different groups have taken the code and tried to create their own versions. Ice IX was one of the first variances and it caused a major problem for banks initially because it was difficult to detect. But we called in the greater anti-malware security community and within a few days they actually had beaten it.

One of the things the banks have done to fight botnets is they've gone after the command-and-control servers of Zeus with Microsoft, and also on our own many times. These command-and-control servers control the Zeus infections themselves and they're also where the data stolen from the devices are dumped. Once we gain access to them, we can see what was stolen, banks can re-issue credit cards or contact the infected people, as we know they're infected, and this went very well for a while.

What happened in the last eight months is a new version called Zeus 3, or Zeus Gameover, came out and it made it much harder to find the command-and-control structures. One thing you'll hear as a general theme from banking and malware is: This is a cat-and-mouse game where we're constantly, slowly escalating with the slow progression. We go after them. They get a little bit better. They beat us for a while. We go after them, and on and on it goes.

One of the bigger threats as of right now is this thing called Citadel. Citadel is derived from Zeus and is adding a lot of powerful new features that make account takeover easy. One of them is what we call the video grabber. The video grabber actually records your keyboard and mouse movements when you interact with their malware so that it can see you as you reach through their phishing form and see where you hesitate, they literally take this back as a QA control, and they reengineer their malware to make that phishing page more realistic and will have a higher conversion rate and it will be more profitable to them.

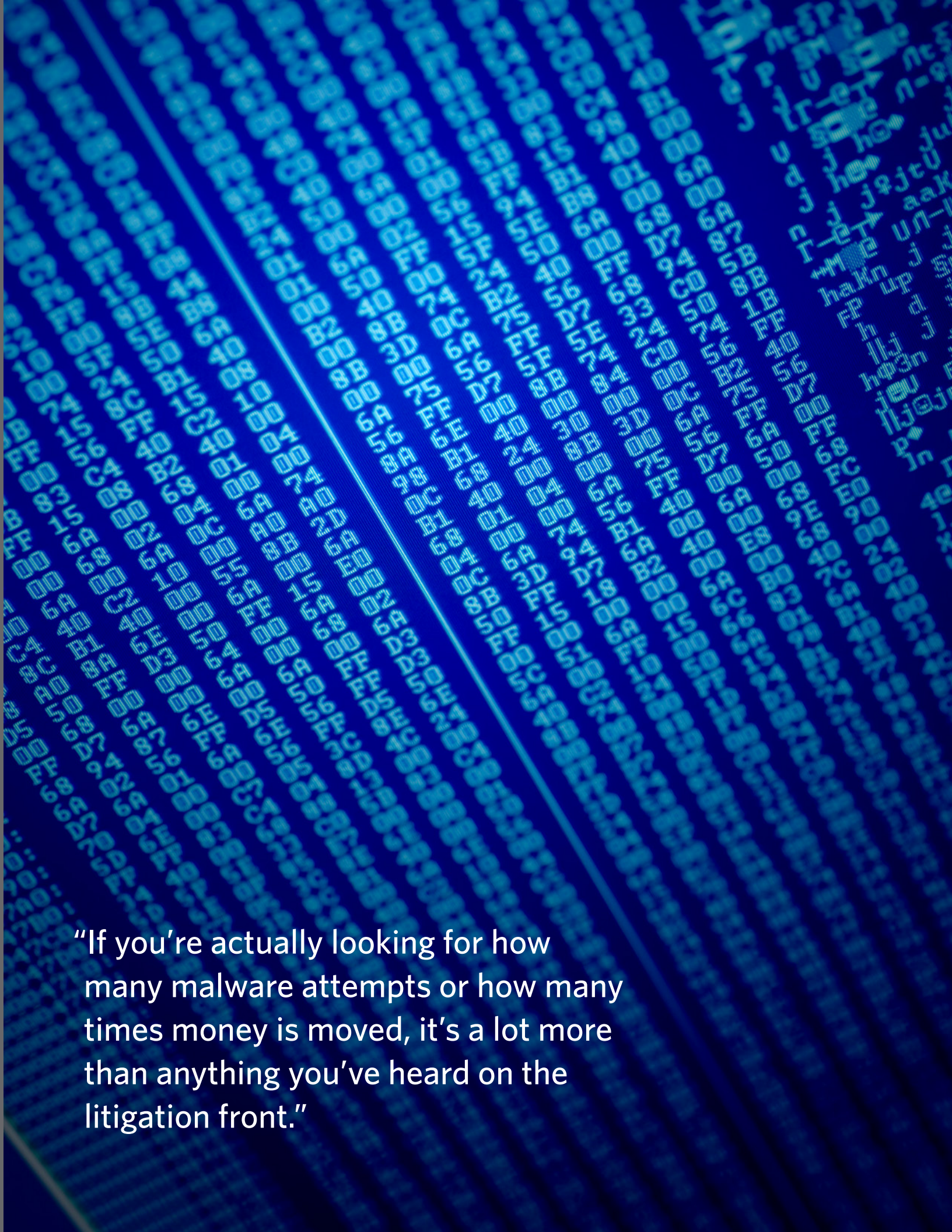
Another thing which is very interesting about this Citadel malware is their language-detection capabilities. The Citadel fraud crew is based in Russia and they do not want to attract the attention of the FSB, which is their version of the FBI. If Citadel malware detects the language on the infected device or the bank is Russian, it deactivates. That stops them from attacking Russian nationals and Russian banks and keeps them safe from too much national attention. They've definitely learned their lesson by going after high-value targets and trying not to be arrested.

We've seen things such as SpyEye that has come and gone. Banks can more easily detect it now, and it's no longer under active development.

Another area which is concerning is mobile malware is definitely growing. We've got Zeus, SpyEye and Citadel. All have mobile smart-phone components called Zitmo, Spitmo, and Citmo, respectively. Banks in Europe have been attacked a lot by these. What they've done is they've focused on out-of-band communications to your phone. They'll either send an SMS message and you must type in

wontok™ SafeCentral

ISMG INFORMATION SECURITY MEDIA GROUP



"If you're actually looking for how many malware attempts or how many times money is moved, it's a lot more than anything you've heard on the litigation front."

"The problem is when you get down to the regional and community banks. There we see a major decline in anti-fraud expertise."

that number to validate the transaction or they use a mobile transactional authentication number [in Europe], which is pretty much a number you enter in to validate the transaction. That goes for your phone.

Now what happened at that point was fraudsters had to figure out, "How do I infect people's phones," because what they wanted to do was get their hands on those numbers. They've come up with Zitmo, Spitmo, and Citmo which is actually part of the infection on your desktop PC. What it does is it links your phone number to them and it forwards all incoming SMS messages from banking institutions only to the fraudster. What actually happens is the bank believes that you've got your transaction number and it definitely must be you, but you never actually get to see it. All mobile phones right now are susceptible, except the Apple ones. However, I really believe that once there's enough financial incentive, no smart device will be safe.

One final thing I want to talk about, which is quite interesting, is fraudsters are now going back to targeting bank executives. They're actually phishing them directly. They hope to infect inside the bank, and then once they're inside the bank they can probe for weaknesses. It's much more like an APT-type scenario, and they also want to be able to impersonate the executives, so they will send e-mails out to them, see all their documents, and that can give them access to privileged data. I see a lot happening.

Incidents Under the Radar

FIELD: We've seen some high-profile court cases in the past couple of years. I'm thinking of ExperiMetal, PATCO certainly which settled this past year. These are the ones that we see. But what types of incidents are occurring that we don't see?

BAYLOR: PATCO, and the companies that appear in litigation, there are two main characteristics. One is they've received major financial loss due to malware, and the bank decided to not reimburse. These tend to be actually the tip of the iceberg. There are actually 11 steps you've got to go through to get money stolen from your account, including: getting infected; being able to move money from your account; you have to have ACH or wires, which is a rapid way of moving money from your bank account; you have to have money mules ready. It's actually very, very complex, and there are also things such as when money moves from your bank, it has to go to a money mule. The money mule has to actually get there and pull the money out, and if the bank is fast enough, it detects the fraud and it can freeze that money. When that money even is pulled out, it has to be cashed and then sent over. There are many, many steps along the way. There are actually 11 steps, and if any one of those is broken, it doesn't happen. If you're actually looking for how many malware attempts or how many times money is moved, it's a lot more than anything you've heard on the litigation front.

Impact of FFIEC Guidance

FIELD: One of the things that we saw in 2011 was the advent of the FFIEC authentication supplement. How has institutions' conformance to this guidance impacted account takeover?

BAYLOR: The FFIEC guidance has definitely caused banks to focus on account takeover. There were things banks were looking at and many in the top ten already have strong anti-fraud programs and they use dozens of detection mechanisms and very, very advanced controls.

The problem is when you get down to the regional and community banks. There we see a major decline in anti-fraud expertise. Many of the smaller banks don't write their own software or use platforms from third parties, and the problem is sometimes those third-party platform vendors don't play well with our security vendors. I've actually seen situations where banks have created great due-diligence, purchased a strong anti-fraud solution that meets the FFIEC guidance, only to see vendors saying they won't implement this.

wontok™ SafeCentral

ISMG INFORMATION SECURITY MEDIA GROUP

"For some of the smaller banks, two or three hits of Zeus and the whole bank is out of business."

Generally, the guidance doesn't raise the bar at the cutting edge of malware, because every single control it mentions can be beaten by this, but the guidance itself acknowledges that. For large banks, it encourages them to layer in controls and make it harder for malware to see. For smaller banks, which have quite honestly been the cash cows for malware, it serves as a great wake-up call. For some of the smaller banks, two or three hits of Zeus and the whole bank is out of business. In their case, infosec has been primarily focused on system IT and compliance needs, but this actually changes them and gets them into the battle against the fraudsters. The FFIEC guidance I would think is more a call to action rather than a "how to beat the bad guys" guide.

Top Takeover Threats

FIELD: A few minutes ago, you talked about the advent of mobile malware and talked about the evolution of other account takeover threats. When you look at the threat landscape, what jumps out to you as the top account takeover threats for this year?

BAYLOR: A think there are really three. As you said, as you put more trust in mobile devices, from a bank's security perspective we're going to put more risk on them. Some banks trust mobile devices more; others less. And mobile banking software for fraud has been available for two years. I think they're waiting for banks to go to the next level of putting more risk, more trust and more cash-moving abilities on these devices, where I think the new malware is already waiting to go, and they're going to consider it a major cash-out.

The second thing is banks themselves are on the target list. Criminals are using botnets and APT methods to penetrate banks and steal information. What they're going to be looking at is what the fraud risk engines are inside the bank. How are they configured and how can we avoid detection? They're aggressively taking the battle inside the banks.

The third thing we will see is more partnering across the criminal ecosystem. About 30 months ago, we were being hit by the Dirt Jumper DDoS attacks, where Zeus would take money from the bank account, usually over a million dollars, and their colleagues would launch a major DDoS attack to take the victim bank offline so that nobody would detect the fraud. Some huge banks are actually getting hit by that, and I think it's the shape of things to come.

wontok™ SafeCentral

iSMG INFORMATION SECURITY MEDIA GROUP

"The FFIEC guidance I would think is more a call to action rather than a 'how to beat the bad guys' guide."

Top Defenses

FIELD: Let's talk about advice to banking and security leaders. You spoke about the FFIEC guidance being a call to action. What are the actions that organizations should take? Where should they invest their time and their money to combat account takeover?

BAYLOR: It's been a great question, especially ever since litigation began and banks realized they must do more. There are really three areas they should look at. The first is procedure, which is, before the account takeover occurs they should examine which customer is a high risk, which one is a single control - which means any one person can send money - which one is ACH and which one is freeform wires where you can send the money to absolutely anyone without notice.

The second thing they should look at is when the account takeover happens, how we minimize the losses. How do we disable the accounts, terminate the sessions, track down where the money goes and freeze it?

The next real area is focused on back-end systems, and these are the fraud detection malware engines. The FFIEC wants them. They can solve many, but not all, of the account takeover problems. Many cost millions of dollars to implement and integrate, require expensive staff to tune, and can take years to implement. And as many banks find, users are not predictable and they can get a lot of false-positives, which if they freeze can result in customer loss and them ending up in court.

Where we really think they should focus on is front-end, or customer-facing, technologies. These are plug-ins or software the bank actually gives to their end customers. Banks have been traditionally sparing in doing this for three reasons. One, they think they're guaranteeing the software will always work, which isn't the case, especially if they carefully word it. Two, they're afraid of blue-screening the devices and they're worried about support cost. The third is they're also worried customer uptake has generally been low, unless you really push users into using it.

What I have seen is there has been a major price change in the last 12 months, and to get it really focusing on procedure and customer-facing technologies. This really adds value more than any other and it can be implemented generally within days rather than six months or a year. At NSS Labs, we focus on products and found vast differences between them: between usability, the ability to defeat malware and the security of the product itself. When you're looking at these devices, price and market share are by no means predictors of value. That's one area where banks need to test the software. By doing that, they'll save themselves a lot of money because the most expensive is definitely not the best, and at the end of the day they'll save their customers from account takeover, which saves everyone a lot of money. ■

LISTEN TO THE INTERVIEW

http://www.bankinfosecurity.com/interviews/account-takeover-2013-outlook-i-1753

wontok™ SafeCentral

ISMG INFORMATION SECURITY MEDIA GROUP

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401
sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com