websense®

iSMG INFORMATION SECURITY MEDIA GROUP

7 Stages of Advanced Threats

Jason Clark, James Robinson of Websense on Key Characteristics

What are the seven stages of advanced threats, and what can organizations do to improve how they defend against them?

Jason Clark and James Robinson of Websense share new insights and strategies.

How does one distinguish advanced threats from traditional? One key difference, says Robinson, security architect and strategy officer at Websense, is that classic threats target systems. Advanced threats are after intellectual property.

"The advanced threats are also getting much more complex," he says. "They're using many steps to actually become successful," including social engineering and software exploits targeting the end-users.

The seven stages of advanced threats account for how threat actors are breaching organizations, as well as the methods they are using to steal data. This information helps security leaders to deploy appropriate controls, says Clark, chief security and strategy officer.

"We look at it as an architecture framework," Clark says. "Now that we've broken down how they're going to get in, how they're going to get the data out and try to evade our security, [then] what's the perfect architecture [to prevent] that?"

Read on to learn from Clark and Robinson:

- Distinguishing characteristics of advanced threats;
- Origin of the seven stages;
- New security solutions.

Robinson is the security architect and strategy officer at Websense. His key responsibilities are internal security strategy and innovation. He brings more than a decade of both IT and product engineering security leadership to Websense. He has previously held leadership positions with Fortune 150 and Fortune 100 companies including: Emerson Electric, Anheuser-Busch and State Farm Insurance.

Clark is chief security and strategy officer for Websense, Inc. In this role, Clark and his team are responsible for corporate strategy, information security, marquee account relationships, and providing strategic services to CIOs and CISOs worldwide. As a former CISO and vice president of infrastructure for Fortune 100 and 500 companies, Clark uses his business and security expertise to advise CXO executives on successful strategies to improve their IT infrastructure.

"That mindset of just focusing on one aspect and not the entire ecosystem is exactly what we've set ourselves up for and what the advanced threat is taking advantage of."

-James Robinson

Advanced Threats vs. Traditional Threats

TOM FIELD: James, what distinguishes advanced threats from traditional threats that organizations have faced?

ROBINSON: There are a couple of different things that really change the game with advanced threats compared to traditional, and there's not really a set definition of what's a traditional threat and what's an advanced threat, but the game is definitely changing, and we're seeing this change over the last couple of years. Traditional threats typically are going after systems, and we didn't see a lot of traditional threats. This would be more like the worms that would propagate, going after the data inside of your systems.

The advanced threats that we're seeing today are really starting to target the information and the intellectual property that you have inside of your organization. The advanced threats are also getting much more complex. They're using many steps to actually become successful, and they're using these steps from traditional threats that we've seen. Things like social engineering, which was a threat all organizations have known for a long time, dealt with and had varying degrees of success with that - that's an aspect of the advanced threat.

Another thing is exploiting software vulnerabilities, which is something that we've known about for a long time as an industry, but now it's actually being included into advanced threats, the different stages and being executed against our end-users. That's one of the different changes as well. In my history of doing penetration tests, I'd always be asked to go and focus on a web server and focus on maybe where the data goes after that, but not focus on the end-users. That approach right there, that mindset of just focusing on one aspect and not the entire ecosystem, is exactly what we've set ourselves up for and what the advanced threat is taking advantage of, where they're targeting the end-users and then going after the data and getting access to this data that they want to steal from the organization.

The other thing the advanced threats are also starting to dive into [are] blind spots. ... Traditional security approaches that we use to secure ourselves, they're also using those to steal the data and to ex-filtrate information from our organizations.

7 Stages of Advanced Threats

FIELD: Jason, let's talk about the seven stages. What's the origin of this seven-stage approach?

CLARK: Probably about five years ago, [we started to] break down how the bad guys are breaking in, what the steps are that they're taking each step of the way as they try to get their hands on our data, and then understanding what the controls are. The seven stages is really more of a fact of, "this is exactly the steps that they're all taking," and we wanted to understand how they're getting around the controls and where do those existing controls we have with technology slide in. How are we being protected?

It hasn't been talked about as the seven stages in the past. Using as an example your home, if [a bad guy] is going to break in, he's going to try to either come through the window; he's going to come through the door. What's the next step you're going to do to invade whatever security you have? It's just the various stages of that.

However, at the same time, we look at it as an architecture framework. Now that we have broken down how they're going to get in, how they're going to get the data out and how they're going to try and invade our security, what's the perfect architecture for that? Because everything else today is very siloed in one stage, or one and a half or two stages, but nothing will look at all seven stages and share information of what's going on and really maintain the state of that bad guy, all the way down from infiltration to ex-filtration. We started then building that technology into our [solutions] as a framework of understanding the need to share that intelligence. Everything we do, this is the framework that we use.

At the same time, we looked at and we got together with a brain trust of the top 30 CISOs in the Fortune 500 that we're friends with and

"It may not be that data theft is occurring while you're on the corporate network, but when you're off the corporate network, when you go home and you work at night."

-James Robinson

looked at this as, "We can take this to another stage and we can really start saying this isn't just about technology." This is about people and processes as well. Since this is the threat model for how the bad guy gets in, we should start doing strategy assessments and grading ourselves on successfulness.

It's a collaboration of knowing this is how it works, how the bad guy gets in and gets stuff out. Then we go to our technology as being aware of that, and at the same time then build a whole strategy and framework around people, process and technology, and a strategy assessment around the seven stages.

Breaking Down the Stages

FIELD: Let's talk about some of these seven stages, and James I'll toss this question to you. Let's start with reconnaissance and lure. What's happening here and how is it happening?

ROBINSON: Reconnaissance and lure are the first two stages of the attack. There are different things that happen here. Reconnaissance is a lot of information gathering. That's the situation where the attacker's starting to put themselves in a position where they want to compromise an adversary or someone else. Tom, if I wanted to compromise you, what I would do is I'd look up your name, I'd look up where you live, I'd look up activities and things that you're involved in so I can then craft a lure one way or another. I could send you an e-mail. I could build a website that maybe you'd be interested in going to, and I'd put these out there with information that's relevant to you with data that you want to actually use.

In *The New York Times* attack, it laid it out very well; they documented things and had all kinds of articles and posts on it. There was the gentleman, David [Barboza]. He was actually putting information out there and then writing an article on China. By doing so, China found out about this. What did they

"It's the volume that's starting to kill us and overwhelm our traditional approaches and defenses."

-Jason Clark

want to do? They wanted to figure out where David was getting his information: what connections did he have; what e-mails; how much information did he have? They targeted David, and they spear-phished an e-mail to him, basically luring him to click on the link inside of that e-mail. That's really what's going on there. They're looking for a target, they're identifying a target, identifying the information and then crafting a message or crafting a way for that person to gain trust in that site or gain interest in it - maybe not even trust, just enough interest - to get them to be baited and run the rest of their attack on that person's systems.

Understanding Exploits

FIELD: Let's talk about the exploit. What's new here?

CLARK: The exploit is something that's interesting. It's something that we've known for a long time - the exploit generation. Things that are changing are not just these vulnerabilities that are now being taken advantage of, but the sheer volume. Before it used to be something that we wanted to share these vulnerabilities, and we wanted to share this vulnerability information with each other. We knew that we could put defenses in place. But now, instead of just finding a software bug that then leads into a security vulnerability, instead of just finding those and sharing them so we can fix them, people are going out and searching for them so they can actually leverage those software bugs, those vulnerabilities, and actually exploit them. The difference now is really that of volume. It's that volume, and now it's being done at a level where they want to find these issues. They want to find these zero-days before anyone else knows about them so they can remain stealthy, so they can execute code on your system, or they can get your system to do things like pull down other variances of malware or drop a file.

Our lab group looks at malware, exploit files and all kinds of different things each day and they detonate these and watch and see what their behaviors are. They find over 1,000 a day that anti-virus doesn't pick up. Now it's the volume that's starting to kill us and overwhelm our traditional approaches and defenses.

The other thing is the exploits are getting much more sophisticated. The exploit and dropper files nowadays are starting to do things like maybe they only execute, call home or do certain things in the hours, times or environments where it's safe for them to do so. They may look and see, "Am I being executed on a VMware stack or some type of virtual stack? Am I off-network or on-network? Am I at home? Am I on a hot spot?" Now they know there's a good chance that traditional capabilities and things that an organization would deploy to protect the company aren't there.

Data Theft

FIELD: James, let's talk about data theft. How do you find that it's evading detection today?

ROBINSON: The main one that we're seeing at this point is the use of SSL. We deployed SSL to help secure us and actually be a mechanism to help protect end-users and help ourselves as a security organization, and those same things are being used against us. It's a double-edged sword where we don't have the visibility. Now exploits, calls home, the ex-filtration of data, that's being done over encrypted channels. So if you don't have visibility into that, you'll never see that data leave.

The other thing is traditional approaches of, "Let's just take an image." I think almost all of us have probably been on a WebEx, a GoToMeeting or something like that, and went ahead and did a screen capture and captured what was on our screen, and now we have that for one reason or another. That same type of mindset and mentality to take a screen shot of it, send it out and it will never be detected is also being used.

As mentioned earlier, now data theft is happening at certain times. It's intelligent where it may not be that data theft is occurring while you're on the corporate network, but data theft would occur when

"The truth is, you get much more effectiveness and return for your money the closer you put your security around what you're protecting."

-Jason Clark

you're off the corporate network, when you go home and you work at night. If you bring up your system, if your approaches, your people, process and technology don't protect you and let you know, "Hey, I'm off network and I need to have a different mindset," or, "I'm off network and I need to have a different control," then you'll never get visibility into that data that's leaving.

CLARK: As you look at the seven stages, and as James just talked through some of the examples - the beginning, the middle and the end of the stages - the most important controls today most people are putting most of them on the perimeter, which is really protecting stages one, two and three. But the truth is, you get much more effectiveness and return for your money the closer you put your security around what you're protecting. The biggest investments really should be closer to the seventh, sixth and fifth stage, instead of one, two and three, which is the opposite today.

I'm a big believer that as the bad guy starts to move down the stages, you actually gain so much more context. In the beginning you would just say, "That's weird. It's the first time we've ever seen this URL. We don't see anything bad yet." But at the time someone could get their hands on the data, you can start saying, "Wait a minute. This data has never tried to leave via SSL to some .com sitting in China." Or, "I know this user has never ever touched this type of data before." Or, "Wait a minute. This user is now raw encrypting this data. Raw encryption is not a standard encryption technology. We use something else." All of a sudden you've got so much more context - who, when, where and how - that you can make better decisions and, unfortunately, an investment or two on the front-end - too much where your pawns are in a chess game and not enough where the king is.

ROBINSON: I'd like to add on that. We were talking to a peer organization of ours and, inside of their company, they feel that they can't put any type of control closer to the end-user or to the client. They need to use network-based controls everywhere, and that's exactly the mindset, exactly what's happening, that's used against us as security organizations because the attackers know that interesting devices are now coming onto the network that we have no control over. They know that systems need to be on our network to allow certain organizations to be creative or maybe do things that we can't control and we can't have visibility into. They know that. They're leveraging that against us.

Human, Technical Resources

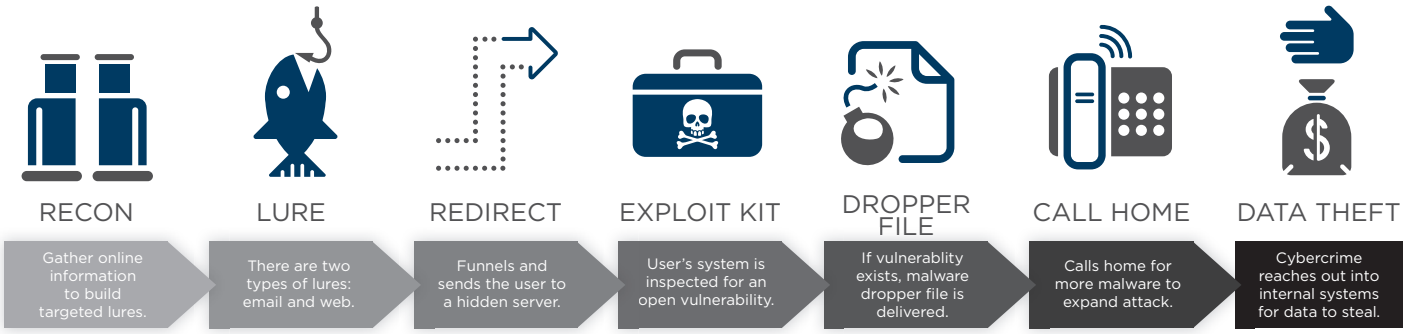
FIELD: James, what human and technical resources do organizations need to support defense against this seven-stage approach?

ROBINSON: What I'll do is I'll break this down into people, process and technology. I'm a true believer in that architectural principle or framework for guiding your controls and what you're trying to achieve. From a technology aspect, there have been some changes lately. The traditional "let's protect our front-end, websense.com," that approach is still a threat that we have to think about.

In the new advanced threat, where they're targeting our end-users, trying to go after the intellectual property and data that we have inside our organization, that changes. That traditional approach isn't going to be as effective in that one threat. How did that change? Now we need to actually look at where this user is going. We need to look at DLP. We need to look at these technologies, help feed into processes and dive into the process piece.

As an organization, we need to be serious about our incident-response capabilities. We need to be serious about having an educational awareness program to let the end-users know [they're] part of this. You're a part of the threat landscape. They're targeting you. They're not targeting my systems that I'm trying to build, protect and deploy. They're targeting you and using you against us. They're doing a divide-and-conquer type of attack on us. You can bring the users in. A lot of times nowadays, you can use gamification, letting users know that they're part of the attack. Even sharing things that have happened inside of the organization [is] very powerful. A lot of organizations just aren't there. They don't have the educational awareness components. They're still using traditional methods for that, where everyone gathers in a room, goes

The Seven Stages of Advanced Threats
and Data Theft



"We need to ... let the end-users know [they're] part of this. You're part of the threat landscape. They're targeting you."

-James Robinson

through a PowerPoint and they're not using these advanced approaches. How do we get people involved? How do we get people to care about this? That's really a big question that we're looking at internal to IT, and we're doing some cool things inside of IT to try to answer that, working with partnering organizations. How do we get people to be part of this? How do we get to know about these processes that normally, if it was on a PowerPoint, they wouldn't remember, they wouldn't care and they would walk out of the room and maybe take a donut with them on the way out? How do we actually get this in front of them and get them to be part of our team?

The other thing on that end-user note is: How do we incentivize? Using gamification, going back to that, how do we actually reward people and get people to be part of this program? Hollywood has done a great job of including hacking and that type of thing. Can we leverage some of those same things? Hacking is a cool concept now. It's something that people want to know more about. It's something that boards of directors are talking about, all the way down to people. Did you hear Facebook got hit? Did you hear that *The New York Times* got hit? Did you hear about those Twitter posts? Those types of things are very powerful for us to leverage and to educate people on. Let them know this is what's happening. Here's what's going on outside, and you could be susceptible to this. That would be probably the sum of it all: People, process and technology are everything you need to focus on.

CLARK: As James said, people and process is really strong. On the people side, imagine you're securing 10,000 of your users and you have a staff of eight. If you could get those 10,000 employees to be a security team member for two minutes of the day, every day, incentivizing to be part of the security team, all of a sudden you have a volunteer army, and your security team and resources just grew a thousand-fold.

The other thing on the technology side I urge everybody is you have to go from that good-enough security mentality, or the compliance security mentality, to be best technology. You need to demand the best at every single thing you buy, unless it's a commodity, unless it's a check-the-box thing, like AV. Those for the most part are check-the-box stuff. But when it comes to malware, when it comes to data protection and it's really the most effective controls you have, you can't just do it [like] the old days.

Back in '06 and '07, I've done this at other companies by picking my favorite AV vendor and said, "The events for the AV, can you wrap in at the same price these other four or five technologies?" I get to check-the-box and I get a bunch of good-enough security for a very cheap price. Or I buy from a guy who's a network player. I buy from Cisco because they're the architecture play so it just makes

"You have to go from that good-enough security mentality, or the compliance security mentality, to be best technology."

-Jason Clark

sense, but that doesn't work anymore. You have to have the best technology and the most effective technology now at each stage.

Defending against Advanced Threats

FIELD: Jason, let's talk about technology. How do you at Websense support your customers' defense against advanced threats?

CLARK: The focus is we have to make them successful. They need to trust us. We have to be their trusted adviser so that they open up and tell us what they're protecting and what they're concerned about. What are their vulnerabilities and their weaknesses so we can sit there, have that conversation and try to develop a strategy for them that's going to be the most effective?

The first step is getting that trust and focusing on ensuring their success, helping them align with their business and helping them align with the executives and tell the executives not the fun stuff, not the, "Oh my gosh; everything is on fire; we might get compromised," but just breaking down, "Here are the threats, the whole threat-modeling stuff we've talked about, and here is where we're at. We're compliant, but here's what I'm worried about today," and then taking that to the technology space and understanding that.

We have developed an advanced threat security architecture that we share and have a lot of other technologies in it. I talked about the 30 CISOs, good friends of ours in the Fortune 500, and we grabbed a CISO that everyday they're successful against advanced attacks. They might have had a compromise, but they've beaten the bad guys out. They're winning in the war. We've mapped how they're winning and we've built this framework that seems to be consistently how the top organizations are winning the war. We're now sharing that framework with our customers, or, for that matter, any head of security in a Fortune 1000 that reaches out to us. We want to share and we want to help the security community be successful together.

This framework breaks down the ten different technologies that they need to do to be successful in the people, process and technology stuff, and try new products at Websense. Our web-security stuff, our threat protection, cloud protection, and the endpoint, the laptops and the mobile devices, as well as our spear-phish protection and our data-theft protection tools, are very, very critical to those Fortune 500 customers. Many of them will tell you it's the secret. It's the number-one way that they're catching the bad guys every single day, whether they're external bad guys or internal bad guys. ■

LISTEN TO THE INTERVIEW

http://www.bankinfosecurity.com/interviews/7-stages-advanced-threats-i-1912

Websense, Inc. is a global leader in protecting organizations from the latest cyber-attacks and data theft. Websense TRITON comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. Tens of thousands of enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices.

websense®

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