

The New Wolves of Wall Street

A new class of cyber criminals is targeting companies' private information.

By: [Michelle Kerr](#) | July 5, 2016



Cyber security measures advanced by leaps and bounds over the past decade. Unfortunately, cyber criminals sharpened their game even more.

As it gets tougher each day to slip in through back doors, hackers turned their talents toward carving out side windows. They adapted, developing new business models and finding smarter ways to profit off of the backs of organizations.

Credit card information, personally identifiable information and protected health information are all still in demand, but they're no longer the only treasures that cyber criminals are after.

“It is no longer hacking merely for a quick payout. It is hacking as a business model.”

— Preet Bharara, U.S. attorney

They want your trade secrets. They want your intellectual property. They want to eavesdrop on your most sensitive financial activities so they can leverage that information on the stock market — shorting stock, investing in stock, timing stock to their advantage.

The cyber security challenge is intense, because it's hard to get a handle on. These crimes are being perpetrated by various groups of actors with different motivations. They're being executed using a broad array of techniques that include any combination of malware, phishing and social engineering.

They could be coming at you from anywhere in the world. And it's not even necessarily your systems that are being attacked directly. It could be your vendors, your partners — any organization that has a connection to your confidential information.

Troubling Numbers

Verizon's "2016 Data Breach Investigations Report" covers cyber incidents affecting organizations in 82 countries and across a myriad of industries. According to the report:

- 89 percent of breaches had a financial or espionage motive.
- 89 percent of phishing attacks were perpetrated by organized crime syndicates.
- 63 percent of confirmed data breaches involved weak, default or stolen passwords.
- 30 percent of phishing messages were opened by the target.

Source: 2016 Data Breach Investigations Report, Verizon, April 2016.

Last August, the SEC filed charges in a fraud scheme involving two Ukrainian hackers who broke into multiple newswire services to steal unreleased corporate earnings announcements. The hackers shared the information with 30 people who traded on it, generating more than \$100 million in illegal profits.

The following November, federal prosecutors disclosed the existence of a sizable worldwide hacking scheme, involving more than 100 people in a dozen countries.

Among the other offenses listed in the 68-page indictment, the crime ring orchestrated elaborate pump-and-dump stock schemes and traded on stolen corporate information, pocketing hundreds of millions along the way.

"It is no longer hacking merely for a quick payout," U.S. Attorney Preet Bharara said in announcing the indictment.

"It is hacking as a business model."

M&As Increase Vulnerabilities

The rise of worldwide M&A activity turned the stock market into a profitable playground for hackers — those working for either side of the transaction or outside parties looking for a way to profit illegally from the transaction.

2015 was record-breaking year for M&As, topping \$5 trillion in volume globally for the first time. Half of the targeted companies were based in the U.S.

2016 is expected to see continued high level of activity. That leaves plenty of opportunities for illegal gains.

“If outsiders are aware of the negotiations going on, they can put upward pressure on the stock.” — Bill Sweeney, chief technology officer, BAE Systems Applied Intelligence

“You can disrupt an M&A a lot of different ways,” said Bill Sweeney, chief technology officer at BAE Systems Applied Intelligence.

“One way is you can publicize that it’s going on sooner than people would like.

“M&A is a very sensitive topic because it’s very price dependent. Companies will walk away from deals because they can’t narrow the gap between \$25 and \$30 dollars a share.

“If outsiders are aware of the negotiations going on, they can put upward pressure on the stock. So when somebody thought they were going to be getting a 25 percent premium [against their stock], but now because of the upward pressure, they’re only getting a 15 percent, why would they sell?”

During a “Cyber Security: The Achilles Heel of M&A Due Diligence,” webinar in April, Brian Finch, a partner with Pillsbury Winthrop Shaw Pittman LLP, outlined the recent case of a company that was courted by international suitors.

The company was certain that it was healthy, but repeated audits showed it operated at a loss. An investigation revealed that the company was under attack, with hackers corrupting information to decrease the value of the company.

When the company value bottomed out, a foreign investor swooped in with a lowball offer.



Will Glass, threat intelligence analyst, FireEye

Even if hackers don’t outright alter the data, they’re still finding ways to leverage it.

“We’ve seen China-based groups ... compromising companies across various industries, stealing information that would give them insight into what the best price for the company might be,” said Will Glass, threat intelligence analyst at FireEye.

“We’ve seen groups that are sponsored by nation states — or that we believe are sponsored by nation states — conducting activity leading up to and even during mergers and acquisitions.”

One high-profile case traced to China was the attempted \$40-billion takeover of Canada’s Potash Corp. by Australian natural resources company BHP Billiton.

While the deal fell through for apparently unrelated reasons, an investigation revealed that a Chinese

effort to derail the deal involved attacks on seven law firms, as well as Canada's Finance Ministry and the Treasury Board.

Those third-party attacks are an area of serious concern in terms of intellectual property and M&As, said Kevin Kalinich, global practice leader, cyber/network risk, Aon Risk Solutions.

"The accounting firms and financial advisers are above average in IT security and protection of confidential information," he said.

"But law firms, surprisingly enough, are below average."

The Human Element

What's complicating matters from a risk management standpoint is that attacks take various forms and are typically multi-layered. Spearphishing and social engineering often play a major role because they are consistently successful, despite companies' attempts to alert employees to the dangers.



"The way of the hacker has always been to go after the industry or the exposure where there's the lowest hanging fruit," said Toby Merrill, leader of Chubb's global cyber risk practice.

And in many companies, that means employees. Even a staffer savvy enough to question a wire transfer request might still be duped by a login scheme that looks innocuous or seems relevant to his job.

"What's happening is that hackers are spoofing emails," said Sweeney.

"They're spoofing CFOs and they're spoofing other C-level executives and pretending to be either a consultant or part of the review process ... trying to extract that sensitive information by [sending] an email that looks like it's from the CEO, that says, 'Hey what's the latest on our deal with company X?' And the guy [replies] but it's not going to the CEO; it's going to the guy who spoofed it."

It's not easy to spot spoofed email, he added.

"It looks like an email from your company, with your header. It looks like it's from your domain. It's only if you open it up and look at the source code that you can see what's being shown is not the actual domain its coming from and if you hit reply it's going to go to somewhere else."

It also works because it's not random. Hackers do their homework and understand how their targets operate. They know when to send emails and who to send them to, and what internal procedures are in place so that they can get around them.

FIN4, a large cyber crime ring tracked extensively by FireEye, was so good at duping people that it didn't even bother using malware.

It focused on capturing usernames and passwords to email accounts. FIN4 would craft convincing phishing lures, most often sent from other victims' email accounts and through hijacked email threads.

Spoofting emails have successfully snared some risk managers, CTOs and CFOs.

According to FireEye's Glass, the group would "send an email to someone in a target company and it would say, 'Hey check out this financial investment forum — there's some guy on here badmouthing the company. You might want to take a look.'"

Hackers set it up so that when the link was clicked, it would request their email login and password in order to view the content. The hackers could then take those login credentials and continue their campaign, both within the organization and laterally to external organizations.

It's worth noting that risk management is directly in the crosshairs for this kind of attack.

C-suite executives, legal counsel and anyone involved in the risk, regulatory or compliance functions of a company are prime targets. If you have any connection to sensitive information, they're looking for a way to get their hands on it.

And experts say that such attacks have successfully snared some risk managers, CTOs and CFOs.

Coverage Confusion

There is plenty that still needs sorting out in terms of the coverage options available to insure against such losses. The toughest pill to swallow, said Kalinich, is that the loss of value is not covered by cyber insurance, nor is it covered by any other type of insurance.



Kevin Kalinich, global practice leader, cyber risk, Aon Risk Solutions

"That's a really important factor," he said.

"The actual value of a trade secret, the actual value of a patent, the actual value of intellectual property, is not covered. [In the case of an M&A loss,] not even a crime policy would cover that."

A D&O policy might be triggered if the stock dropped following a failed M&A, but a company would be challenged to relate the event to a cyber hack, or to quantify the impact of the hack on the failed transaction, experts said.

Still, said Kalinich, there are certainly losses that could be covered by cyber insurance, especially if an attack were to result in business interruption, or if it caused damage to the system that required remediation, or forensic investigation.

Culture of Awareness

At a minimum, any company engaging in mergers or acquisitions activity should separate that information from the rest of the corporate environment, said experts. M&A activity should have a segmented network and a dedicated file server, and all documents should be encrypted.

BAE's Sweeney also recommended that related communications with people outside of the organization be restricted to a VPN for added security.

Additionally, all third-party involvement should receive a high level of scrutiny.

Said Sweeney, “You’ve got to look at everybody who’s going to have access to the information, and say, ‘When was the last time you had a cyber assessment? How can we make sure that you’re not going to be the conduit through which people find out this information?’

“That’s where people are getting hacked,” he said. “They’re not getting hacked right in the center. They’re getting hacked by the people on the periphery who are trying to do their best.”

Internally, Glass said, it’s a good practice to follow the law of least access — give people access to the information that they need to do their jobs and nothing more. But that’s just a start.

Hackers figured out that humans are easier to crack than code, so comprehensive staff training should be the foundation of a solid cyber security strategy.

Some companies use internal phishing campaigns to help manage the human side of the risk. Employees who are duped and click on bogus links are redirected to a page revealing their mistake and letting them know they’ll be required to do mandatory extra training.



Nick Rossman, senior program manager, threat intelligence, FireEye

Experts universally agreed that these risks cannot be foisted onto the laps of IT or risk management alone. Boards must be educated and involved, and there must be enterprise-wide collaboration for a company to develop any level of effective defense against cyber espionage.

Make sure you’re speaking the board’s language, said Nick Rossman, senior program manager, threat intelligence with FireEye. “They don’t care about malware, they just want to know what you’re asking them to invest.

“So I think it’s easiest when you have a big scope of data and a partner who can get you a strategy forecast” to help justify decisions about investments, he said.

“In the past, [IT and data systems] were considered kind of a back-office priority, kind of like having enough printer toner or enough chairs,” said

FireEye’s Glass.

“It was an enabling function of the company but not really core to the business. Now every company is an IT company whether they realize it or not.

“Maybe Coca-Cola keeps its recipe in a safe somewhere, but everybody else, for the most part, is keeping their information online or in databases or even in the cloud, because the efficiencies that can be derived from that model are so great.

“In order to make sure that those efficiencies continue, we’ve got to make sure that companies are looking at all the risks inherent with putting all of that information online.” &

Toxic Butterfly

A group first dubbed Wild Neutron, then Morpho and finally Butterfly, is one of a rising number of complex, skilled and highly organized professional crime rings.

Known to be in operation since at least 2011, Butterfly is known for targeting corporate intellectual property of publicly listed companies, most of them in the Fortune 200.

As of July 2015, 49 different organizations across 20 nations, were known to have been hit by the group, including Twitter, Facebook, Apple and Microsoft. Most of the attacks occurred following news reports of potential mergers or press releases about product launches.

In 2013, Butterfly targeted technology companies, then turned its attention to legal and pharmaceutical firms. By 2015, Butterfly was gunning for commodity companies — oil, natural gas, and mining.

Researchers believe that Butterfly is not a nation state-sponsored operation. According to Symantec, the group appears to be run by an organized crime ring with possible U.S. ties.

Based on reports from victims that have chosen to share details with security researchers, Butterfly's primary objective is gaining access to R&D-related computer systems.

What sets Butterfly apart is its ability to flutter away without a trace. After obtaining its target, it cleans up after itself by deleting, rewriting and then re-deleting critical malware files multiple times. In certain cases, the group even used external servers to conduct attacks, avoiding detection by paying for the hardware in small batches of Bitcoin transfers from multiple accounts.

Butterfly appears to have gone dormant since July. But the threat remains. In November 2015, Kudelski Security published a report on a group it called the Sphinx Moth, which appeared to correspond to the activities of Butterfly. Kudelski said it expected the group to undergo a change in its tactics, techniques and procedures. &

—By Michelle Kerr



A group dubbed Butterfly has accessed the sensitive files of at least 49 organizations, most of them Fortune 200 companies.