

Malware intelligence system helps organizations share threat information

EurekAlert!

Safety in numbers

As malware threats expand into new domains and increasingly focus on industrial espionage, Georgia Tech researchers are launching a new weapon to help battle the threats: a malware intelligence system that will help corporate and government security officials share information about the attacks they are fighting.

Known as Titan, the system will be at the center of a security community that will help create safety in numbers as companies large and small add their threat data to a knowledge base that will be shared with all participants. Operated by security specialists at the Georgia Tech Research Institute (GTRI), the system builds on a threat analysis foundation - including a malware repository that analyzes and classifies an average of 100,000 pieces of malicious code each day.



Georgia Tech Research Institute researchers examine analytics data from their new Titan malware intelligence system. Shown are research scientists Andrew Howard and Christopher Smoak, and graduate research assistant George Macon.

"As a university, Georgia Tech is uniquely positioned to take this white hat role in between industry and government," said Andrew Howard, a GTRI research scientist who is part of the Titan project. "We want to bring communities together to break down the walls between industry and government to provide a trusted, sharing platform."

Members contributing information will do so anonymously so other members won't know which specific organizations have been attacked. GTRI will independently verify information provided to Titan and carefully vet the members of the community before they are allowed to participate.

"People tend to think that if an organization gets hit, it was because they had poor security measures," said Christopher Smoak, a GTRI research scientist who heads up the Titan project. "That's not necessarily true, because a variety of factors contribute to intrusions. But until we get to the point that there's no longer a stigma attached to having an infiltration, people are going to want anonymity to participate."

In addition to receiving information about attacks and responses at other organizations, members will receive quick reports on malware samples they submit. Based on what they have learned from the malware repository and by reverse-engineering malicious code, GTRI researchers will be able to provide information on the potential harm from an attack, the likely source, the best remedy for it and the risks to the organization.

"We hope to provide information about the trends that organizations can expect to see, and help them prioritize what they should do to address the risks," said Howard. "We have a significant system behind the scenes to facilitate the exchange of information."

Titan will be especially valuable to smaller organizations that lack the resources to operate their own security evaluation labs, though all members will benefit from sharing information. GTRI information security researchers collaborate with the Georgia Tech Information Security Center (GTISC), which expands the depth of knowledge.

"GTRI will maintain the shared resources that companies can use to help solve their own problems," Smoak noted. "We'll have many organizations contributing to this community, and everyone getting information out; it will really benefit everyone."

Companies today have two primary concerns about malicious software, Howard said. The first is for the loss of intellectual property, such as plans for a new product or bidding documents for a major project. The second is a compromise of the web infrastructure that many companies rely on to do business.

Titan will also help companies educate their computer users about such risks as spear-phishing, which uses email that appears to be from a trusted colleague or friend to trick users into taking a risky action, such as opening an infected attachment. The system will alert companies to the newest threat trends so they can warn their users, and identify the IP addresses that malicious software is communicating with.

"Spear-phishing is very difficult to defend against, because all it takes is one person clicking on something that lets malware into the network," Smoak said. "It's difficult to train a large workforce with varying skill sets to identify the very small nuances that indicate these emails are malicious."

GTRI has been analyzing the malware attacking Windows-based computers for years. Now the analysts are seeing an increase in malicious code designed for Android-based devices – and for Macintosh computers, which previously hadn't been high-priority targets.

"We see Android malware in its infancy right now," said Smoak. "We see what it is doing and how it is working, and we can draw parallels to what we saw earlier with the Windows-based malware. We can probably expect to see the Android and Mac malware follow a similar path."

Malware intelligence system helps organizations share threat information

Published on Electronic Component News (<http://www.ecnmag.com>)

The danger may be especially great for the users of computer systems that previously had not worried much about malware.

"For Macintosh systems, the threats are starting to get scarier," Howard said. "When more malware authors shift their focus to this platform, a lot of people who thought they were safe by not using the Windows OS will be caught off-guard."

Titan now includes half a dozen Fortune 500 members, along with other government and nonprofit organizations. Smoak and Howard have been getting feedback from those members as they've built the system, which will be formally launched in a few months.

"We are looking for additional industry partners to help us use the tool and help refine the system," said Howard. "We believe that members of this community will come together to help each other strengthen defenses."

A determined hacker will probably succeed in compromising most corporate computer networks, but the researchers believe Titan can help companies make that as difficult as possible.

"You may not be able to completely prevent an attack, but you can have a higher wall and stronger defense," Howard said. "Hackers tend to go after the low-hanging fruit, so they will attack the companies that are the easiest to attack. We believe that our community can help all the members strengthen their defenses."

Source URL (retrieved on 12/27/2014 - 5:12pm):

http://www.ecnmag.com/news/2012/05/malware-intelligence-system-helps-organizations-share-threat-information?qt-recent_content=0