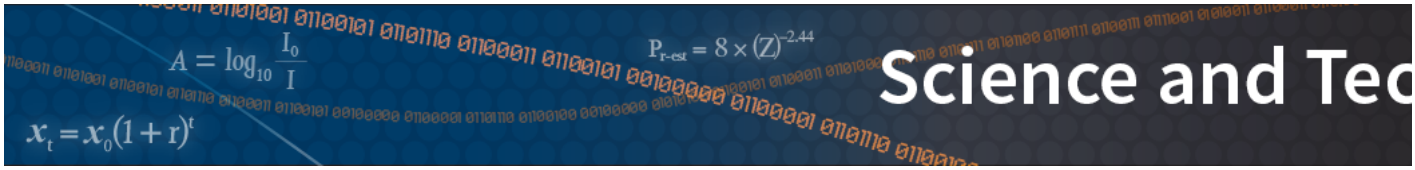

Science and Technology

Snapshot: Dissect Cyber alerts small businesses targeted by cybercriminals

Release Date: May 2, 2017

Cybercriminals are an insidious lot, constantly launching new schemes to steal money from individuals and companies. In the United States, millions of people and small businesses fall victim to internet crimes each year. Most small businesses do not have ready access to timely cybersecurity notifications of possible threats.

Financial loss from cybercrime is a significant and under-reported problem, the FBI's Internet Crime Complaint Center (http://www.ic3.gov) (IC3) has found. The IC3 2015 Internet Crime Report (https://pdf.ic3.gov/2015_IC3Report.pdf) reveals losses of nearly $1.1 billion across the U.S. from 127,145 internet crime complaints. Yet these staggering losses are just the tip of the iceberg. The IC3 report notes that only 15 percent of fraud victims report internet crimes to law enforcement.

To reduce losses from cybercrime, the DHS Science and Technology Directorate (S&T) Cyber Security Division (CSD) funded a new research initiative focused on the best way to alert small businesses to potential threats. The project, Dissect Cyber, is being led by a threat analyst training and alert provider with of same name. CSD is part of S&T's Homeland Security Advanced Research Projects Agency.

The initiative's goal is to develop validated strategies to increase the effectiveness of cybersecurity notifications to companies supporting critical infrastructure sectors, including the U.S. government. The research project, part of CSD's overarching Internet Measurement and Attack Modeling (/csd-imam) (IMAM) project, provides no-fee, early notifications of possible internet-based scams to help minimize damage and loss to companies registered to do business with the U.S. government and listed on the System for Award Management (http://www.sam.gov) (SAM) database.

"Through its research project, Dissect Cyber is providing very timely notifications that help small- to mid-sized companies from falling victim to well-targeted and executed internet and email scams," says IMAM Program Manager Dr. Ann Cox. "In most cases, the Dissect Cyber research provides these notifications to targeted companies before the cybercriminals can launch their schemes. These advance notifications enable companies to take steps to avoid being victimized."

Dissect Cyber monitors new internet domain registrations for web-domain spoofing that could match criteria for Business Email Compromise (BEC) scams. A BEC is a sophisticated scam that targets businesses working with foreign suppliers or that regularly perform wire transfer payments. The scam compromises a legitimate business e-mail account either by spoofing (sending an email using a forged address) or hacking the account.

These scams are gaining traction at an alarming rate. Since January 2015, losses from BEC scams have increased 1,300 percent, with business victims spread through all 50 states and 100 countries. In that time, 22,143 domestic and international BEC scam victims were swindled out of more than $3 billion, the IC3 report finds.

The Dissect Cyber cybersecurity notification team provides a highly specific and yet complimentary service to small businesses listed in the SAM database. When Dissect Cyber detects that a company's internet domain has been spoofed, the cybersecurity notification team—comprised solely of military veterans—calls the affected company to deliver the details of the threat and also follows up with an email notification detailing how to defend against the threat. To date, Dissect Cyber has made more than 3,500 calls with impressive results and successes to show for their work.

Companies that have been notified of a possible BEC scam through CSD's Dissect Cyber research project have avoided falling victim to internet criminals.

For example, at one company a senior employee received an email request for a $26,000 wire transfer from someone posing as the CEO. The hoax email arrived shortly after Dissect Cyber had notified the company of a potential BEC scam. The employee recounts what unfolded next: "We went along for one reply, enough to get the amount and bank details. Then we contacted the local FBI field office, filed an IC3 report and submitted the info to InfraGard (/redirect?url=https%3A%2F%2Fwww.infragard.org%2F). I contacted the parties involved in hosting the domain and the account was terminated. This morning the domain was available and we snagged it."

The head of another company turned down Dissect Cyber's assistance, explaining that his IT department had the company covered. He called back within hours, saying: "I stepped out into the hall and ran into my finance person, who was headed to the bank to get a certified check in response to the fraudulent email you told us was coming!"

In addition to BEC scams, Dissect Cyber also notifies firms registered on the SAM database when their employee logins have been stolen and circulated on the internet by cybercriminals. It even finds the owners of abandoned websites that are being used to distribute ransomware and works to have the sites taken down.

Currently, Dissect Cyber employees contact 30 percent of companies targeted by look-a-like domains within five hours of a fraudulent domain's registration and 93 percent of targeted companies are notified in less than 24 hours. Dissect Cyber is scaling up for round-the-clock notifications by hiring and training additional employees, with a goal of 90 percent notification in less than two hours and 100 percent notification within 24 hours.

"If your company is contacted by Dissect Cyber, heed its warnings and act on its advice to safeguard it," said Cox. Doing so could mean the difference between losing thousands of dollars to internet scammers or beating them.

The Dissect Cyber project will be presented at the 2017 Cyber Security R&D Showcase and Technical Workshop (/redirect?url=http%3A%2F%2Fbit.ly%2FCyberShowcase17), which is scheduled for July 11-13 in Washington, D.C.

Topics: Cybersecurity (/topics/cyber-security)