West Texas Cyber Security Consortium

SPOTLIGHT ON SECURITY

Hackers Paint Bull's-eyes on Cybercurrencies

By John P. Mello Jr.
TechNewsWorld
05/19/14 12:53 PM PT

As last week's attack on Doge Vault indicates, cyberthieves are salivating for cybercurrencies. "Digital currencies are attractive to cybercriminals for a couple of different reasons," said JD Sherry, vice president of technology and solutions at Trend Micro. For one thing, they can use the currencies anonymously to buy cyberweapons and other illegal products and services on the Dark Web.

Another digital currency was brought to its knees last week when the administrators of Doge Vault had to suspend operations after they discovered their online wallet service had been attacked by hackers.

Following an investigation of the incident and the reconstruction of some of their damaged information from a backup, the administrators contacted users.

"After salvaging our wallet, we have ascertained that around 280 million Dogecoins were taken in the attack, out of a total balance of 400 million kept in our hot wallet. 120 million Dogecoins have been since recovered and transferred to an address under our control," they said.

"It is believed the attacker gained access to the node on which Doge Vault's virtual machines were stored," they continued, "providing them with full access to our systems. It is likely our database was also exposed containing user account information; passwords were stored using a strong one-way hashing algorithm."

The Dogecoin attack is another example of how digital currencies are beginning to attract hacker attention.

"Digital currencies are attractive to cybercriminals for a couple of different reasons," JD Sherry, vice president of technology and solutions at Trend Micro, told TechNewsWorld.

"One, they can use those currencies -- when they acquire them through theft and other nefarious activities -- anonymously to buy cyberweapons on the Dark Web."

Mobile Malvertising

Also making digital currencies attractive to Net vermin is the growing acceptance of byte bucks by online retailers.

"Overstock.com is estimating it's going to do (US)$10-$15 million dollars in bitcoin transactions this year," Sherry said.

"So it's attractive not only to put bitcoin mining malware on users' machines but then use it to buy from online retailers accepting it," he noted. "They're going where the money is -- and that includes attacking the digital currency exchanges."

Digital currencies were among the new hacker targets identified in TrendLabs' first-quarter security roundup released last week. Another was point-of-sale terminals at retail chains like Target and Nieman Marcus.

Mobile users continue to attract the attention of digital desperadoes, too. However, the popularity of an old standby -- premium service texting -- has been waning, according to the TrendLabs report.

"Premium service abusers -- the most common Android threat type in 2013 -- no longer topped the Android threat list this quarter," it notes.

"Adware surpassed premium service abusers in terms of volume, possibly due to a recent announcement made by major carriers on dropping premium-text-service-billing rates after acknowledging that these could end up in cybercriminals' hands," the report points out.

"Viewing premium service abusers as less 'profitable' attack tools, therefore, cybercriminals set their sights on spreading adware instead to victimize more users," it adds.

Iranians Change Tactics

Up to now, Iran's answer to Stuxnet, which put a severe crimp in its nuclear development program, has been to vandalize Western websites and mount some distributed denial-of-service attacks on banks and such. That may be changing, though, according to a report released last week by FireEye.

"We believe we're seeing an evolution and development in Iranian-based cyberactivity," the report says. "In years past, Iranian actors primarily committed politically motivated website defacement and DDoS attacks. More recently, however, suspected Iranian actors have destroyed data on thousands of computers with the Shamoon virus, and they have penetrated the Navy Marine Corps Intranet, which is used by the U.S. Navy worldwide."

While not all Iranian hackers have changed their ways, a group that FireEye calls the "Ajax Security Team" has.

"There is a subset of Iranian hackers who are spear phishing targets and using malware to collect information," Ned Moran, a co-author of the report, told TechNewsWorld. "Traditionally, Iranian hackers have conducted attacks designed to garner public attention."

At this point, the scope of the Iranian problem remains murky.

"How widespread this change is is not clear," Moran acknowledged. "How many Iranian actors are engaged in similar transitions is unclear. We can only talk about what we observed, and that's this Ajax Security Team."

Retailers Circle Wagons

A series of mammoth data breaches have rocked the retail industry in recent months, and last week it decided to do something about it. A bunch of retailers under the umbrella of the Retail Industry Leaders Association established a clearinghouse to share and analyze cyberthreat information.

Among the backers of the e Retail Cyber Intelligence Sharing Center are American Eagle Outfitters, Gap, J. C. Penney, Lowe's, Nike, Safeway, Target, VF Corporation and Walgreens.

"The fact that some of these big huge brands are stepping up to the plate, recognizing retail cyberintelligence and actually sharing this information, is a great thing," Chris Strand, senior director for compliance at Bit9, told TechNewsWorld.

"A lot of these corporations are competing with each other," he said. "That's been a huge hindrance to them formulating solutions and sharing solutions between each other."

Sharing information within an industry vertical can be very useful in thwarting criminal behavior, added Brandon Hoffman, a senior director at RedSeal Networks.

"Cybercrime has become quite sophisticated, and targeted attacks are typically executed against certain industries," he told TechNewsWorld.

"Due to the nature of targeted attacks, specialized malware and attack techniques will be developed for focus on an industry," he continued. "Sharing the information related to these attacks -- malware artifacts, spear phishing email campaigns, inappropriate network traffic -- with each other will only make the response and preparation by security personnel that much more effective."

Breach Diary

- May 13. FireEye reports discovery of Iranian hacker group called the "Ajax Security Team," which has been targeting U.S. defense companies and Iranian dissidents with cyberespionage attacks.
- May 13. European Union Court of Justice rules that people can request Google delete sensitive information about them in its search results.
- May 13.Doge Vault, a digital currency provider, suspends operation of its website after reporting it had been attacked by hackers.
- May 13. Paytime, a Pennsylvania payroll company, issues notices to an undisclosed number of customers that it discovered a data breach on April 30. Corporate bank accounts and employee personal information are at risk, the company said.
- May 13. National Institute of Standards and Technology announces guidelines for agency technologists and industry engineers on how to bake security into critical systems.
- May 13. Privacy International files complaint accusing UK's Government Communications Headquarters (GCHQ) of installing hacking programs on millions of computers, mobile phones and webcams to secretly record communications and capture other sensitive information such as user names, passwords, emails and text messages.

- May 13. Microsoft releases optional security updates for its .NET framework that prevents RC4 encryption from being used in TLS connections. The RC4 algorithm is considered vulnerable to NSA attack.
- May 13. Facebook reports 58 percent of the notification emails it sends users are protected by the STARTTLS protocol, which hardens messages against wholesale snooping by well-financed adversaries.
- May 14. Retail Industry Leaders Assn. announces center for sharing cybersecurity information among retailers.
- May 14. Google announces plans to require its Google Apps users to verify their identity with a text message if the company detects a suspicious login attempt.
- May 14. Politico Pro expands its subscription service with launch of Pro Cybersecurity, a coverage area dedicated to online security and privacy news for both private and public-sector policy professionals.
- May 15. Electronic Frontier Foundation releases its fourth annual "Who Has Your Back" report, with comprehensive information on 26 companies' commitments to fighting unfair demands for customer data.
- May 15. BillGuard lanches personal finance app for Android devices that includes alerts when a payment card is involved in a data breach.
- May 15. Security researcher Nik Cubrilovic identifies vulnerabilities in Australian government website myGov that places at risk the personal information of some 2.2 million citizens.

Upcoming Security Events

- May 20. Meeting on Commercial Use of Facial Recognition Technology. 1-5 p.m. ET. Held by National Telecommunications and Information Administration at American Institute of Architects, 1735 New York Ave. NW, Washington, D.C.
- May 21. What's News in PCI DSS 3.0. 11-11:45 a.m. ET. Webinar sponsored by CyberArk. Free with registration.
- May 21. Houston SecureWorld. Stafford Centre, 10505 Cash Road, Stafford, Texas. One Day Pass: $165; SecureWorld Plus, $545; exhibits and open sessions, $25.

- June 3. Meeting on Commercial Use of Facial Recognition Technology. 1-5 p.m. ET. Held by National Telecommunications and Information Administration at American Institute of Architects, 1735 New York Ave. NW, Washington, D.C.
- June 5. Cyber Security Summit. Sheraton Premiere, Tysons Corner, Va. Registration: $250; government, $50.
- June 5. Portland SecureWorld. DoubleTree by Hilton, 1000 NE Multnomah, Porland, Ore. One Day Pass: $165; SecureWorld Plus, $545; exhibits and open sessions, $25.
- June 6-7. B-Sides Asheville. Mojo Coworking, Asheville, NC. Fee: NA.
- June 6-7. B-Sides Cape Town. Dimension Data, 2 Fir St., Cape Town, South Africa. Fee: NA.
- June 14. B-SidesCT. Quinnipiac University-York Hill Campus, Rocky Top Student Center, 305 Sherman Ave, Hamden, Conn. Fee: NA.
- June 18. Cyber Security Brainstorm. Newseum, Washington, D.C. Registration: Government, free; through June 17, $495; June 18, $595.
- June 20-21. Suits and Spooks New York City. Dream Downtown hotel, 355 West 16th St., New York City. Registration: Before May 6, $299; after May 6, $549.
- June 21. B-Sides Charlotte. Sheraton Charlotte Airport Hotel, 3315 Scot Futrell Dr., Charlotte, NC. Free.
- June 21-30. SANS Fire. Hilton Baltimore, 401 W. Pratt St., Baltimore. Courses: by April 30, $1,249-$4,695; by May 14, $1,249-$4,845; after May 14, $1,249-$5,095.
- June 24. Meeting on Commercial Use of Facial Recognition Technology. 1-5 p.m. ET. Held by National Telecommunications and Information Administration at American Institute of Architects, 1735 New York Ave. NW, Washington, D.C.
- June 27-28. B-Sides Manchester (UK). Reynold Building, Manchester University (M1 7JA). Free.
- Aug. 2-7. Black Hat USA. Mandalay Bay, Las Vegas. Registration: through June 2, $1,795; through July 26, $2,195; after July 26, $2,595.
- Aug. 7-10. Defcon 22. Rio Hotel & Casino, Las Vegas. Registration: $220.
- Sept. 17-19. International Association of Privacy Professionals and Cloud Security Alliance Joint Conference. San Jose Convention Center, San Jose, Calif. Sept. 18.

Cyber Security Summit. The Hilton Hotel, New York City. Registration: $250; government, $50.

- Sept. 29-Oct. 2. ISC2 Security Congress 2014. Georgia World Congress Center, Atlanta. Registration: through Aug. 29, member or government, $895; non-member, $1,150. After Aug. 29, member and government, $995; non-member, $1,250. ECT

John Mello is a freelance technology writer and contributor to *Chief Security Officer* magazine. You can connect with him on Google+.

http://www.technewsworld.com/story/80475.html