Weak Cybersecurity Helps North Korea Raise Money

One source of cyber attacks is highly motivated to continue – because it needs the money.

Meet North Korea, recently discovered to be rather cracking good at hacking into systems. Its state-sponsored hackers are succeeding in raising millions of dollars for the rogue country, often reported to be broke, due to tightening economic sanctions.

According to many news reports, hackers with ties to the country are working hard to earn bitcoin, steal bitcoin – or just plain steal assets they can convert to bitcoin.

Bitcoin is not controlled by any government entity nor easily traced. With the United Nations and others forbidding trade or world aid going to N. Korea due to its nuclear weapons efforts, Kim Jong-un's regime has resorted to "creative financing" through cyber attacks.

The attacks are assumed to be "state-funded" because most N. Koreans aren't allowed to access the Internet, according to cybersecurity expert Dorothy Denning. Internet access is only available to "elites and foreign visitors" via a connection through China, (and more recently, through Russia, according to Bloomberg Business News.)

"Would-be hackers can't launch attacks across borders; they can't even pick up hacking manuals, code and tips from the many online forums that other hackers in other nations use to learn the trade and share information," Denning wrote in an article published Feb. 20 on TheConversation.com (https://www.imagequest.com/denning-korea/). "On top of that, N. Korea maintains exceptionally strong controls over its population."

The article also cites a report by South Korea's defense agency, which claims N. Korea employs 6,000 people for cyber warfare and cyber attacks. Several news organizations say many of these alleged hackers were university-trained in Pyongyang, with some outlets naming N. Korea's University of Automation.

continued on P.02
Are You Compliance Audit –Ready?
Lack of Preparation Could Be Costly

If your firm handles protected health information or works with organizations that do, you may face a regulatory audit of your IT Compliance posture and a review of the Business Associate Agreement you should have signed.

It’s not just the obvious hospitals, health care practices, and other medical firms that must adhere to HIPAA. Anyone doing business with them will have some contact with the protected health information (PHI) they possess, and they will fall under the federal HIPAA regulations.

Other regulations govern the protection of personal financial data and general personally identifiable information (PII). Most are federal regulations you must follow or face fines.

ImageQuest has extensive experience with regulatory audits such as those from the U.S. Office for Civil Rights (OCR) which governs HIPAA, the Federal Financial Institutions Examination Council (FFIEC) which prescribes uniform principles and standards for many community banks, and others.

“We know what they are looking for, and what best practices to follow,” said Milton Bartley, Co-Founder, President & CEO of ImageQuest. “Often there is a deadline attached to the audit which firms may find stressful and hard to meet. Potential gaps in procedures and processes could be very costly to you and your regulated client.”

Bartley added: “You should assume an audit is in your future, so the time is now to prepare for it and correct any deficiencies. Contact ImageQuest to discuss our Audit Response Services as soon as possible.”

continued from P.01

Most attacks attempt to trigger physical and psychological paralysis in S. Korea, including causing problems for S. Korea’s military and national infrastructure.

But the country is accused of attacking other targets too, including Sony Pictures in 2014, and the Bangladesh Central Bank in 2016. The Sony hack was widely believed to be retaliation for the movie “The Interview,” which put N. Korea’s leader in a bad light.

The bank hack was all about the money. Similar attacks, using the same malware, were reportedly attempted on other banks as well. The U.S. has said N. Korea tried to steal $1 billion from the New York Federal Reserve last year; a spelling error tripped them up.

Several news outlets have reported on an apparent North Korea-based group of hackers known as “Lazarus.” Law enforcement implicated “Lazarus” in the WannaCry ransomware epidemic last spring.

Last fall, several news outlets reported on an apparent N. Korea-based group of hackers known as “Lazarus.” Law enforcement implicated “Lazarus” in the WannaCry ransomware epidemic last spring, and it suspects Lazarus to continue to be very active in ransomware attacks, including attacks uncovered last fall.

Those recent attacks attempted to steal data as well as victims’ processing power to mine bitcoin. The malware behind these attacks had traits that suggested a common source.

And it will continue. The New York Times reported in October that intelligence officials estimate that N. Korea “steals hundreds of millions of dollars a year from ransomware, digital bank heists, online video game cracking, and more recently hacks of S. Korean Bitcoin exchanges.”

It’s a cyberwar – and we recommend you don’t help out the N. Koreans with weak cybersecurity – or by paying the ransom.

If your firm handles protected health information or works with organizations that do, you may face a regulatory audit of your IT Compliance posture and a review of the Business Associate Agreement you should have signed.

At ImageQuest, we know referrals are an important part of creating and building business relationships. Great leads can come from anyone at any time.

Why not explore this opportunity and receive benefits for you and your company?

It’s easy to join our referral program, and it’s a great way to earn additional income while helping companies benefit from ImageQuest’s vast IT services and support.

- If your Managed IT Services referral becomes a recurring client, you or your favorite charity will receive $1,000.
- If your Managed Compliance referral becomes a client, you or your favorite charity will receive a $100 amazon gift card.

WHAT WOULD MAKE A GOOD REFERRAL?
A company in any professional industry with at least 20 computers or anyone with a regulatory compliance component to their organization.

HOW DO I SUBMIT A LEAD?
Simply call Milton Bartley or Jay Mallory at 888.979.2679 or email leads@imagequest.com
www.imagequest.com/referral-program
**PA city struggles to contain expensive malware attack**

Allentown, Pa., may spend “close to a million” dollars to recover from an ongoing attack by a version of the Emotet malware.

Emotet is known as a very advanced “polymorphic network worm” designed to steal banking and other log-in credentials. It injects malicious computer code into a victim’s computer then spreads past anti-malware defenses by constantly changing. Emotet gets on a network through phishing emails with malicious documents in emails disguised as an invoice or other Word or PDF attachment. Sometimes the emails direct the victim to a URL link where the malware downloads to their system. In Allentown, the malware has been “self-replicating, stealing credentials such as passwords for city employees,” reported the Allentown Morning Call newspaper. It forced the city to shut down financial and public safety operations.

Mayor Ed Pawlowski said at a Feb. 20 council meeting that the city hired Microsoft for $185,000 to “triage” the attack, which had already been underway for a week. “This is an incredibly costly fix for us. We’ll probably have to spend close to a million dollars just to get it fixed and put something in place so that this doesn’t happen again,” Pawlowski told the council. “We’re in triage mode. We haven’t gotten to corrective mode.”

Several cybersecurity firms sent out an alert in November about Emotet, with Sophos noting that the malware “takes advantage of weak admin passwords to help (it) spread across a victim’s network.” Sophos also noted that “stopping this worm requires every machine on an infected network to be protected with an antivirus” program.

“This virus is unique,” Pawlowski told the council. “It actually has intelligence. … So it bypasses and evades any of our anti-viral firewalls that we have.”

Added city IT Director Matthew Leiber: “This is not Ransomware. This could be worse.”

When asked by a councilman if Microsoft could “guarantee” its work would prevent future malware attacks, an unnamed Microsoft representative at the meeting responded that no one could make such a guarantee, “not even three-letter agencies that protect our national security.”

The Microsoft representative also said that while the city “had a lot of tools in place” to protect itself, “there are some architectures we’re going to change, (and) there may be some other tools we’ll make some recommendations on. Maybe budgeting reasons primarily are why (the tools) are not there right now.”

---

**MEET OUR TEAM**

**DEMARCUS BROWN** is an IT Support Specialist II – and one of the calm, friendly voices you hear when you call ImageQuest for help. Callers may have log-in issues, printer issues; their desktops or laptops aren’t booting up. And they may be nervous or stressed by the problem. That stress doesn’t transfer to DeMarcus. He knows he can usually fix the problem quickly. It helps that he’s very patient. “Treating people like a human being is probably the key to the whole thing,” he says. DeMarcus pursued his degree in computer systems networking and telecommunications because he found it interesting and a way to help people. “I could learn something other people don’t take the time learn,” he said. “A lot of people don’t want to do this. But I can really help people.”

DeMarcus said he enjoys his work at ImageQuest. “I love it here,” DeMarcus said recently. “It’s definitely a family atmosphere here.”

Hear directly from DeMarcus himself at https://www.imagequest.com/meet-demarcus/

---

**MEET A CYBER CRIMINAL**

Alexsey Belan, 30, is accused of conspiring to breach Yahoo in 2014. Authorities believe two Russian FSB agents hired Belan to find accounts belonging to Russian journalists, and Russian and U.S. government officials, among others. The Yahoo breach compromised 500 million accounts. Belan also has been indicted for hacking Zappos.com, in 2012, and Evernote and Scribd in 2013. Forbes said he specializes in cracking Word Press websites and called him “one of the more adept website hackers working across the Russian cybercrime underworld.”

Born in Latvia, Belan has Russian citizenship. His aliases include “Magg,” “M4G,” “Moy.Yawik,” and “Quarker.”

There is a $100,000 reward for information leading to his arrest.
Check Us Out!

OUR LIVE EVENTS

Mar 6  "Ransomware, Inc." presentation, co-sponsored by Hyland Insurance, Louisville.


April 20 “Your Biggest Cybersecurity Threat is Hiding in Plain Sight” panel moderator, Kentucky Society of Certified Public Accountants (KYCPA) Spring Business Conference, Louisville.

May 22 “Ransomware, Inc.” presentation, BKR International Americas Regional Meeting, Dominican Republic.

From Our Customers

“Thanks for hanging in here for such a long time to complete the problem with software vendor!”

“DeMarcus was friendly and listened and addressed the issues I was having and also set up our emails as timely as possible. Great experience!”

“Very helpful and quick resolution to my computer issue!”

Tamika “was great. She got the job done quickly and was so pleasant to talk to on the phone. You need to pay her (well). My day had not been going too well, and she got me in a much better mood with her kindness and just the sound of her voice.”

“ImageQuest knows their stuff!! I was in panic mode when I notified ImageQuest. My server went berserk, and I did not know what to do. I talked with Stephen. He did not panic and stayed in control mode. I had a meltdown. He assured me it would be ok. It was ok. He recovered my documents and stayed calm throughout my issues. Thank you, Stephen!”

“Lee and Jay came in to help us with the moves. It went smoothly. Thanks.”

“Angela was wonderful and very thorough.”

“Everyone one is so polite!!”

“Brad is so smart and patient too! Thank you!”

Thank YOU to our clients who shared their positive feedback about our help. We appreciate your sharing this feedback with us! You can read more comments on our home page – just click on Read Client Comments.

If you are not having this experience with your Technology Vendor, maybe you should give us a call!

WELCOME NEW CLIENT!


Cardinal Carryor is a 70-year-old forklift sales and service organization. Cardinal Integrated Systems sells and services other warehouse equipment, such as conveyors, pallet racks, docks, cranes, and security cages.

Cardinal Integrated Systems also provides planning, engineering, and project management services, according to the company website.

https://www.cardinalcarryor.com/

Both companies operate under one roof in Louisville, Ky., with a satellite office in Bowling Green, Ky., and employ a total of 104 people.

Cardinal has thrived thanks to UPS’s International air hub in Louisville, and the tremendous growth of regional warehouse operations the hub supports. The Materials Handling Equipment Distributors Association named Cardinal Carryor a “Most Valuable Partner” for 2018.

Cardinal Carryor has had a long relationship with ImageQuest Senior Security Analyst Lee Walton and considers him “a very valuable resource to Cardinal Carryor,” said Cardinal President and CEO Brad Baker. “Our industry has been hit with ransomware in recent years, and that is very much on my mind.”

“Lee understands our business,” Baker said. “Lee has gone above and beyond – and I trust Lee.”