College of Information Studies

University of Maryland Hornbake Library Building College Park, MD 20742-4345

Networked Malware

Session 37

INST 346

Technologies, Infrastructure and Architecture

Ex-contractor says he hacked into U-Md. databases to alert others to security flaws

By Dana Hedgpeth and Nick Anderson April 10, 2014 Email the author

A former contract worker for the University of Maryland said he hacked into scores of databases in the school's computer system and posted the university president's "private information" online to draw attention to security problems.

David Helkowski, 32, has been linked to a security breach in March that involved accessing student grade-point averages and student and employee Social Security numbers and contact information, as well as exposing the Social Security and cellphone numbers of university President Wallace D. Loh. In February, there was a larger security breach of roughly 300,000 sensitive records of names, Social Security numbers and birth dates of students and staff and faculty members. Helkowski has not been accused of involvement in that breach.

Helkowski told the Baltimore Sun that he saw flaws in the university's system even before February's breach and that he brought up his worries but grew frustrated. He has not been charged with a crime and told the Sun that he considers himself a whistleblower.

SQL Injection Attack

SELECT * FROM users WHERE name = ' ' OR '1'='1';

statement =

"SELECT * FROM users WHERE name = ' " + userName + " ';"

' OR '1'='1

Cyberthreats

- Attack vectors
  - SQL insertion
  - Access control compromise
- Attack goals
  - Hijacking
  - Defacing
  - Denial
  - Extortion
  - Theft
  - Damage

An Access Control Failure

The Sarah Palin email hack occurred on September 16, 2008, during the 2008 United States presidential election campaign when the Yahoo! personal email account of vice presidential candidate Sarah Palin was subjected to unauthorized access. The hacker, David Kernell, had obtained access to Palin's account by looking up biographical details such as her high school and birthdate and using Yahoo!'s account recovery for forgotten passwords. Kernell then posted several pages of Palin's email on 4chan's /b/ board.

A hacker who claims to have broken into the AOL account of CIA Director John Brennan says he obtained access by posing as a Verizon worker to trick another employee into revealing the spy chief's personal information.

The hacker, who says he's under 20 years old, told WIRED that he wasn't working alone but that he and two other people worked on the breach. He says they first did a reverse lookup of Brennan's mobile phone number to discover that he was a Verizon customer. Then one of them posed as a Verizon technician and called the company asking for details about Brennan's account.

Using information like the four digits of Brennan's bank card, which Verizon easily relinquished, the hacker and his associates were able to reset the password on Brennan's AOL account repeatedly as the spy chief fought to regain control of it.

The documents they accessed included the sensitive 47-page SF-86 application that Brennan had filled out to obtain his top-secret government security clearance. … The applications, which are used by the government to conduct a background check, contain a wealth of sensitive data not only about workers seeking security clearance, but also about their friends, spouses and other family members. They also include criminal history, psychological records and information about past drug use as well as potentially sensitive information about the applicant’s interactions with foreign nationals—information that can be used against those nationals in their own country.

Researchers from the Atlanta-based cybersecurity firm Dell SecureWorks reported that the emails had been obtained through a data theft carried out by the hacker group Fancy Bear, a group of Russian intelligence-linked hackers that were also responsible for cyberattacks that targeted the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC), resulting in WikiLeaks publishing emails from those hacks.

SecureWorks concluded Fancy Bear had sent Podesta an email on March 19, 2016 that had the appearance of a Google security alert, but actually contained a misleading link—a strategy known as spear-phishing. (This tactic has also been used by hackers to break into the accounts of other notable persons, such as Colin Powell). The link—which used Bitly, a URL shortening service—brought Podesta to a fake log-in page where he entered his Gmail credentials. The email was initially sent to the IT department as it was suspected of being a fake but was described as "legitimate" in an e-mail sent by a department employee, who later said he meant to write "illegitimate."

Cyberthreats

- Attack vectors
  - SQL insertion
  - Access control compromise
- Attack goals
  - Hijacking
  - Defacing
  - Denial
  - Extortion
  - Theft
  - Damage

Browser Hijacking

As Ars Technica first reported on Friday, users on social media started complaining earlier this week that YouTube ads were triggering their anti-virus software. Specifically, the software was recognizing a script from a service called CoinHive. The script was originally released as a sort of altruistic idea that would allow sites to make a little extra income by putting a visitor's CPU processing power to use by mining a cryptocurrency called Monero. This could be used ethically as long as a site notifies its visitors of what's happening and doesn't get so greedy with the CPU usage that it crashes a visitor's computer. In the case of YouTube's ads running the script, they were reportedly using up to 80 percent of the CPU and neither YouTube nor the user were told what was happening.

We Are Anonymous.

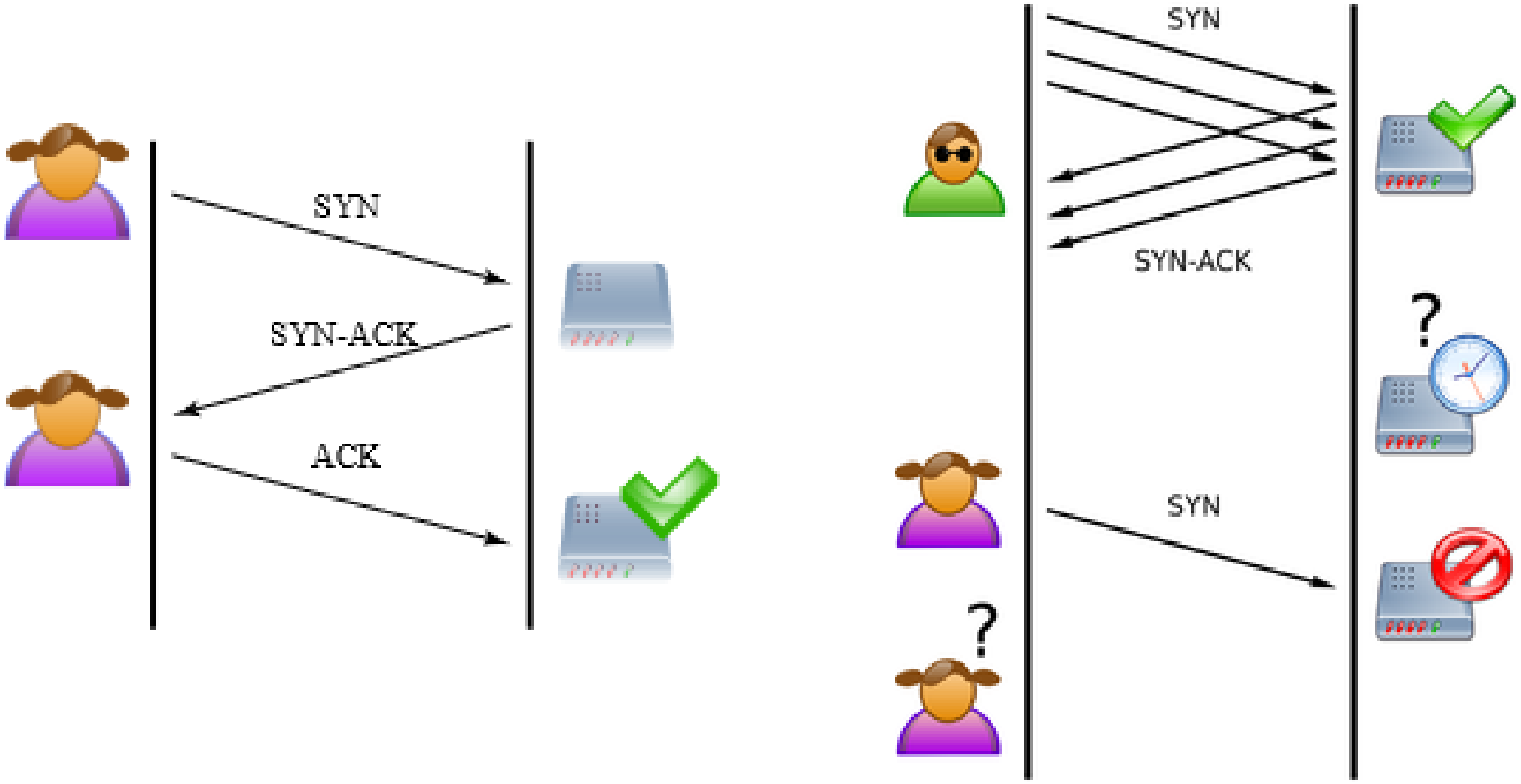
We Are Legion.

We Do Not Forgive.

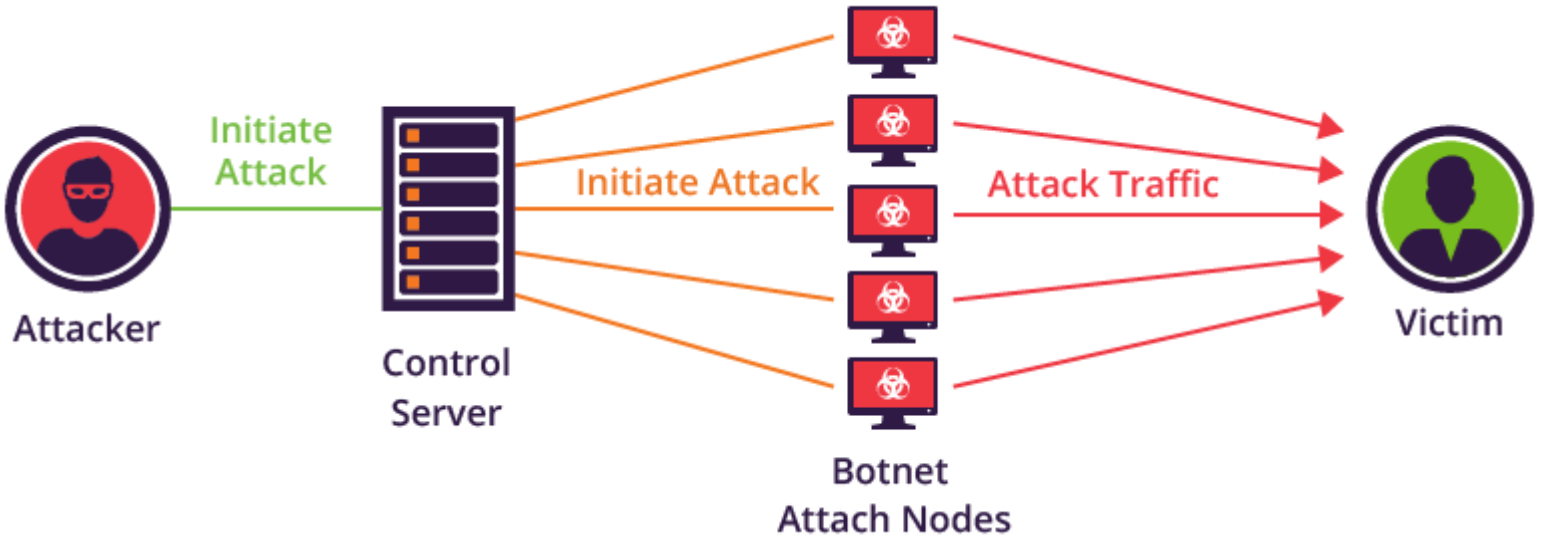
We Do Not Forget.

Expect Us.

Denial of Service (DoS): SYN Flood Attack



Botnet Distributed DoS (DDoS)



CryptoLocker

Your personal files are encrypted!

Private key will be destroyed on
9/24/2013
6:21 PM

Time left

54 : 15 : 15

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

In July 2015, a group calling itself "The Impact Team" stole the user data of Ashley Madison, a commercial website billed as enabling extramarital affairs. The group copied personal information about the site's user base and threatened to release users' names and personally identifying information if Ashley Madison would not immediately shut down. On 18 and 20 August, the group leaked more than 25 gigabytes of company data, including user details.

Passwords on the live site were hashed using the bcrypt algorithm. Due to a design error where passwords were hashed with both bcrypt and md5, 11 million passwords were eventually cracked.

A $101 million theft from the Bangladesh central bank via its account at the New York Federal Reserve Bank was traced to hacker penetration of SWIFT's Alliance Access software, according to a New York Times report. It was not the first such attempt, the society acknowledged, and the security of the transfer system was undergoing new examination accordingly. Soon after the reports of the theft from the Bangladesh central bank, a second, apparently related, attack was reported to have occurred on a commercial bank in Vietnam.

Both attacks involved malware written to both issue unauthorized SWIFT messages and to conceal that the messages had been sent. After the malware sent the SWIFT messages that stole the funds, it deleted the database record of the transfers then took further steps to prevent confirmation messages from revealing the theft. In the Bangladeshi case, the confirmation messages would have appeared on a paper report; the malware altered the paper reports when they were sent to the printer. In the second case, the bank used a PDF report; the malware altered the PDF viewer to hide the transfers.

Your Car Can Drive You

In 2015, security researchers Charlie Miller and Chris Valasek hacked into a 2014 Jeep Cherokee and managed to “turn the steering wheel, briefly disable the brakes and shut down the engine,” the Post’s Craig Timberg reported. The pair found they could also access thousands of other vehicles that used a wireless entertainment and navigation system called Uconnect, which was common to Dodge, Jeep and Chrysler vehicles. The hack prompted Fiat Chrysler to recall 1.4 million vehicles.

Cyberthreats

- Attack vectors
  - SQL insertion
  - Access control compromise
- Attack goals
  - Hijacking
  - Defacing
  - Denial
  - Extortion
  - Theft
  - Damage