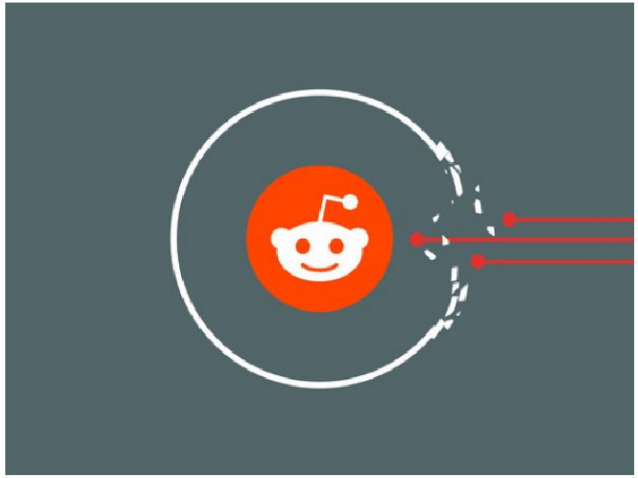
IT security.
This is where we are...
Where are we going with this?

LILY HAY NEWMAN SECURITY 08.01.18 04:38 PM

REDDIT GOT HACKED THANKS TO A WOEFULLY INSECURE TWO-FACTOR SETUP



CASEY CHIN

REDDIT SAID IN a blog post Wednesday that a hacker broke into the company's systems in June and gained access to a variety of data, including user emails, source code, internal files, and "all Reddit data from 2007 and before." And it likely could have been avoided if some Reddit employees were using two-factor authentication apps or physical keys instead of their phone numbers.

wired.com

15.08.2018. Riga

@KirilsSolovjovs

SamSam: The (Almost) Six Million Dollar Ransomware

sophos.com

Key Findings

- SamSam has earned its creator(s) more than US$5.9 Million since late 2015.
- 74% of the known victims are based in the United States. Other regions known to have suffered attacks include Canada, the UK, and the Middle East.
- The largest ransom paid by an individual victim, so far, is valued at US$64,000, a significantly large amount compared to most ransomware families.
- Medium- to large public sector organisations in healthcare, education, and government have been targeted by SamSam, but our research discovered that these only make up for about 50% of the total number of identified victims, with the rest comprising a private sector that has remained uncharacteristically quiet about the attacks.
- The attacker uses care in target selection and attack preparation is meticulous. SamSam waits for an opportune moment, typically launching the encryption commands in the middle of the night or the early hours of the morning of the victim's local time zone, when most users and admins would be asleep.
- Unlike most other ransomware, SamSam encrypts not only document files, images, and other personal or work data, but also configuration and data files required to run applications (e.g., Microsoft Office). Victims whose backup strategy only protects the user's documents and files won't be able to recover a machine without reimaging it, first.
- Every subsequent attack shows a progression in sophistication and an increasing awareness by the entity controlling SamSam of operational security.
- The cost victims are charged in ransom has increased dramatically, and the tempo of attacks shows no sign of slowdown

coindesk.com

Crypto Mining CEO Said to Disappear With $35 Million In Funds

Nikhilesh De
Jul 30, 2018 at 16:15 UTC | Updated Jul 30, 2018 at 16:20 UTC

NEWS

The chief executive of a cryptocurrency mining startup has reportedly disappeared with $35 million in client investments, Newsweek reported Monday.

Le Minh Tam, head of Vietnam-based Sky Mining, has been missing since July 26, according to the report. The startup, which claimed it would rent crypto miners to investors for between $100 and $5,000, received funds from roughly 5,000 individuals prior to Tam's disappearance last week. Each miner would promise a 300 percent return over a year, with investors keeping the machines for at least 15 and up to as many as 18 months.

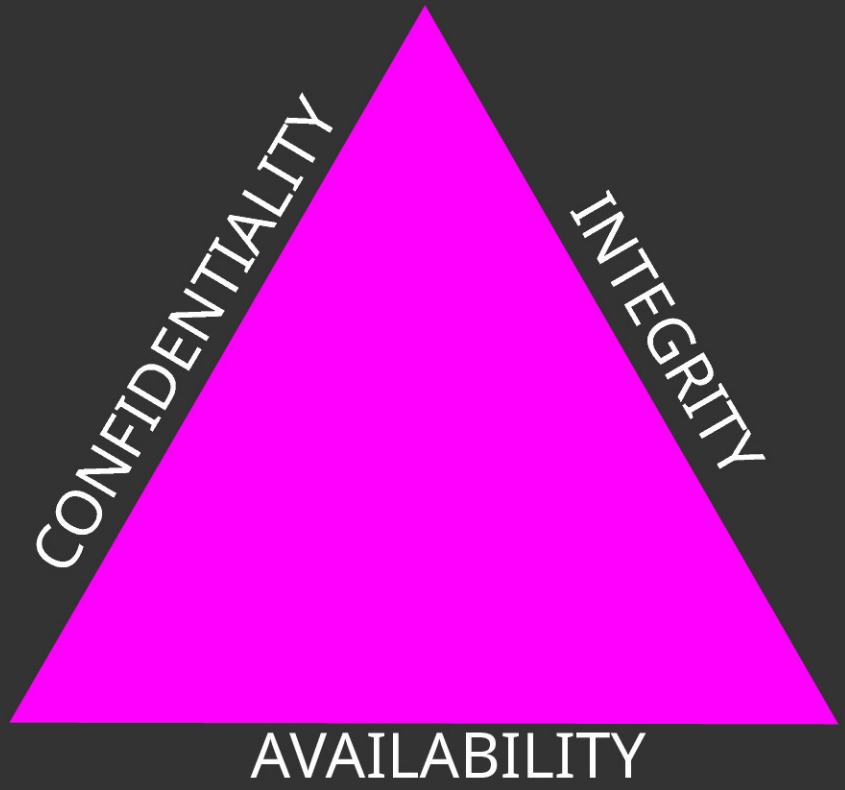
However, when one group of investors went to pick up their miners last Friday, they found that the firm's mining facility and office were empty, and that the mining machines had already been taken away. Tam later reportedly claimed he sold them to cover financial losses, and that his disappearance was aimed at protecting his life.

IT security.

¿ Security ?

- Safety – the state of being free from harm
- Security – the measures used to protect against adverse events
- Information Security – the practice of protecting information
- Information Technology Security – the practice of securing the used technologies (to advance Information Security)
- Cybersecurity – the practice of securing a specific part of cyberspace

Information Security



This is where we are...

Internet (1983)

- No commercial interests
- No specific need for security tools
- A parallel reality
- Hacking happens
  - fun, friendly, playful

Internet (1983)

Organizations targeted:

- Telcos
- Computer industry
- Academia

.com bubble (1995-2000)

- Internet (esp. Web) becomes a commodity
- Attracts businesses
- For marketing at first
- Online sales follow soon

The hats (pre-2000)

Cyberdefence (2007, Estonia)

Cyberdefence (2009, Latvia)

Where are we going with this?

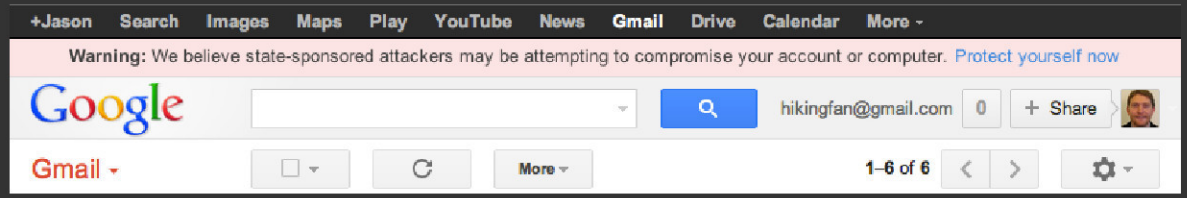
Ransomware

- Ransomware is getting more prevalent
- Ransom amount is increasing

- Users should be using unconnected backups
  - but it's hard (even though it isn't)

State cyberattacks

- State-on-state cyberattacks affect you too



- Companies sometimes cave to the pressure and provide backdoors or other kind of access to oppressive or hostile governments
  - while they should be the protector of the users for user places their trust in them

Surveillance

- There is pervasive surveillance both on-line and in real life

- Businesses and municipalities use surveillance to provide safety and increased profits
  - but they don't give a damn that users are forged into products in the process

IoT

- We're being attacked by the Internet of Things
- Botnets everywhere!

- Manufacturers should be making more secure devices
  - but there are no incentives
- Users should not be buying unneeded, insecure devices
  - but they don't care

Hackers

- Hackers still hack you:
  - random choice
    - script kiddies, joyriders
  - high value
    - competitors, organized crime
  - collateral damage
    - state attackers and others
- Users should use strong security and be vigilant
  - but they fall for social engineering and other attacks due to lack of education
- Bad guys should be afraid of punishment
  - but border-less nature of the Internet and its anonymity often prevents that

In summary

- Internet is turning into wild wild west
- Thus regulation and heavy policing is imminent
- Brace yourself!
- Use the time we have left for unimpeded growth of your business!

IT security.
This is where we are...
Where are we going with this?

Reach me at:
http://kirils.org
kirils@possiblesecurity.com