Portsmouth Computer Group
Cyber Security Workshop

10/28/18

pcgit
Advanced IT Support

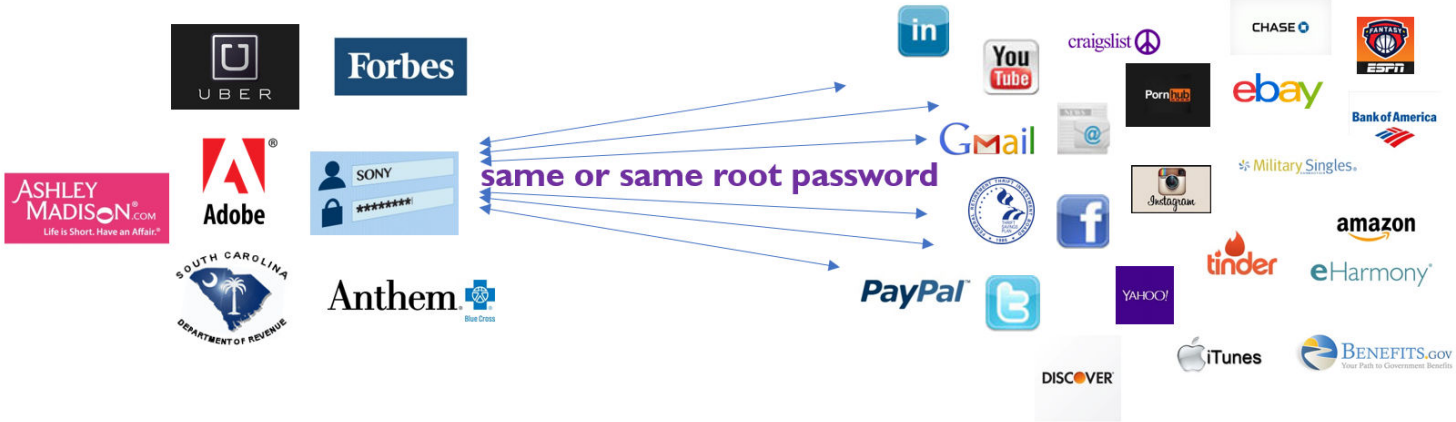
Cyber crime is on the rise

- **80%** of hacking-related breaches leveraged either stolen passwords and/or weak or guessable passwords
- **85%** of businesses with <1000 employees have been hacked, and *most don't even know*
- **4.2 BILLION** email account credentials and **85 MILLION** stolen PII records (drivers license, SSN, DOB, etc.) a for sale on the Dark Web

pcgit Advanced IT Support

DARKWEB ID

The human factor is key



76% of people will use the same password for most, if not all, websites

pcgit
Advanced IT Support

Small Businesses at great Risk

"…data stolen from businesses ends up on the dark web where criminals buy and sell it to commit fraud, get fake identity documents, or fund their criminal organizations."

"…information available for sale on the dark web is up to 20 times more likely to come from an entity whose breach wasn't reported in the media. Many of these are smaller retailers, restaurant chains, medical practices, school districts, etc. In fact, most of the breaches the U.S. Secret Service investigates involve small businesses."

Federal Trade Commission, 2017

pcgit
Advanced IT Support

The Costs are Staggering

- Global cost of data breaches will reach **$2.1 TRILLION** by the year 2019
- **73.18%** of US Population with at least 1 compromised credential found within the Dark Web: **(237,736,346)**
- **18.6%** Percent of US Population with a compromised social security number found within the Dark Web: **(60,441,444)**

How Are Credentials Compromised?

Phishing
- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

Malvertising
- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

Watering Holes
- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

Web Attacks
- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

pcgit
Advanced IT Support

Data is Sold at Auction

Typical price range on Dark Web markets for compromised credentials, ranging from online services to corporate network usernames and passwords

$1-$8

For those who make credentials available on the Dark Web, the financial rewards can be significant. A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing them. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

pcgit
Advanced IT Support

Protecting Against Credentials Compromise

While there is always a risk that attackers will compromise a company's systems through advanced attacks, the fact is that most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only through defense in depth - implementing a suite of tools such as security monitoring, data leak prevention, multifactor authentication, improved security awareness and others - can organizations protect their credentials and other digital assets from seeping onto the Dark Web.

"For [attackers targeting] big corporate networks, persistence and focus will get you in without a zero day; there are so many more vectors that are easier, less risky, and more productive."

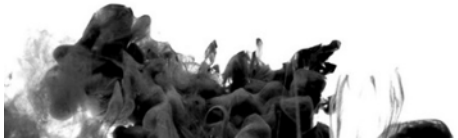
pcgit
Advanced IT Support

We can help

- We now offer **Dark Web ID** – a threat monitoring tool that provides **24/7/365** monitoring for signs a company's exposed and compromised email credentials.
- The platform's engine scours millions of sources including:

  botnets ☠ criminal chat rooms ☠ peer-to-peer networks
  malicious websites and blogs ☠ bulletin boards ☠ illegal black market sites

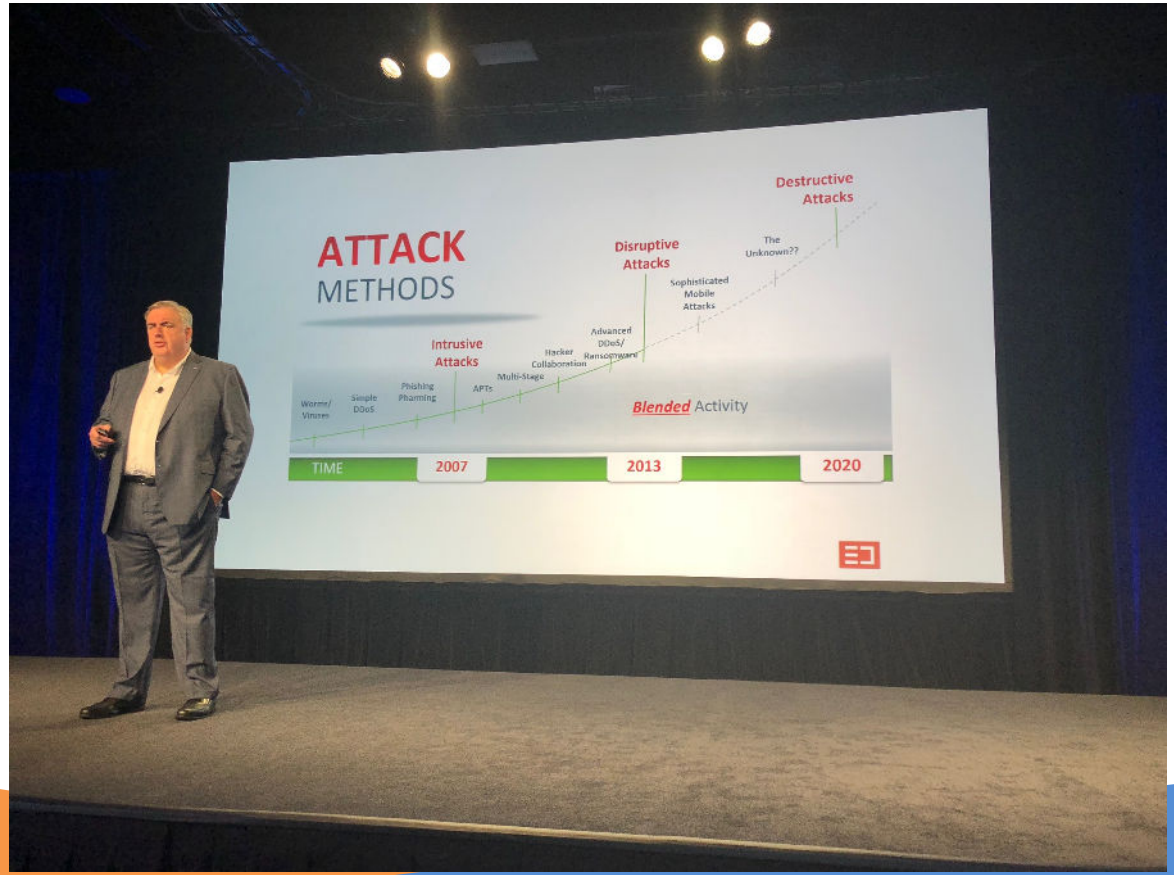
- And other private and public forums – all to ensure we know as soon as compromise occurs.



We go into the Dark Web, so you don't have to.

pcgit Advanced IT Support

How will your prepare?



How will your prepare?

- Planning
- Policy “AUP”
- Collaboration
  - Partners, Vendors, Industry Experts
- Technology
- Make sure you are prepared for an Emergency
  - Process, People, Vendors, Clients, Employees

HR Acceptable Use

- How can you expect your employees to know what is acceptable on their own?
- Have the discussion at the time of employment.
- Update your “AUP” on what your organization wants for a baseline
- PCG can add more detail as neededed

Security Layer Offerings

- **Foundation Layer**
  - Server and PC monitoring and remediation
  - Webroot AV
  - Backup. BDR
  - Firewall
  - Password Policy
  - Computer and Server security updates

Included with your SLA

Security Layer Offerings

- **Security Plus**
  - Profile and Detect
  - DNS “Web Content Filtering”
  - Security Awareness Training / Phishing
  - CISCO AMP/IDS
  - Dark Web “Password Comprimises”

Security Layer Offerings

- **Security Advanced**
  - Detect and Respond
  - SOC “Security Operations Center
  - SIEM. Event Tracker
    - Compliance
  - Sentinel One (Advanced AV, self healing, roll back)
  - 2 Factor Authentication

Security

- You’re part of the team
- If you see something, say something
- Be cautious. Better safe than sorry
- PCG is always here for questions or concerns, email help@pcgit.com or call 603-431-4121