BCNET 2019

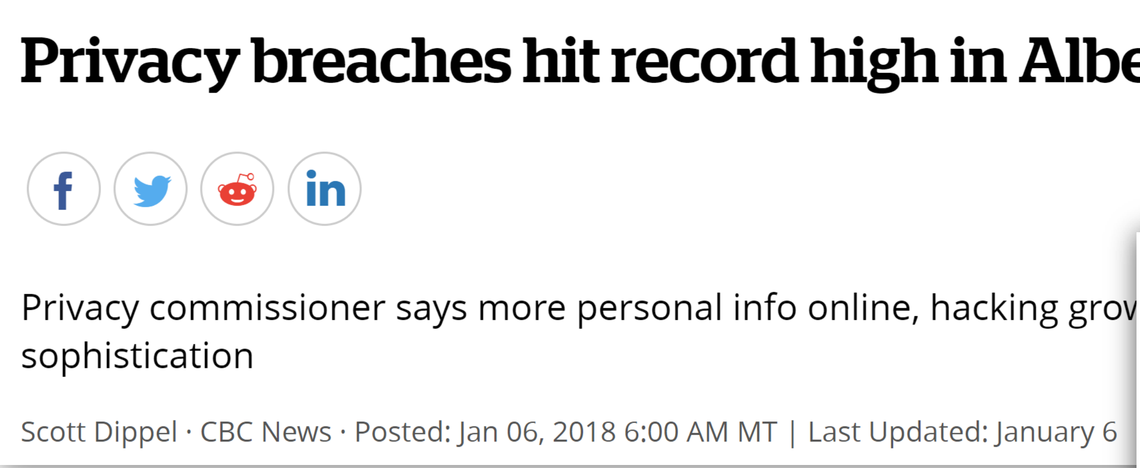
Exploited!
Seeing through the eyes of a hacker

Michael McDonnell, CISM, GCIA, GCWN, MLIS
michael.mcdonnell@vcura.com
https://linkedin.com/in/itpromichael

I am a Cybersecurity Consultant

- CISM, GCIA, GCWN
  - Certified Information Security Manager
  - Certified Intrusion Analyst (GCIA)
  - Windows Security Administrator
- B.Sc. and MLIS
- 1990s
  - Virtual Schools & Web Development
- 2000s
  - Web Development, Library IT
  - Post-Secondary Cybersecurity
- 2010s
  - Cybersecurity: Training, Assessment, Architecture

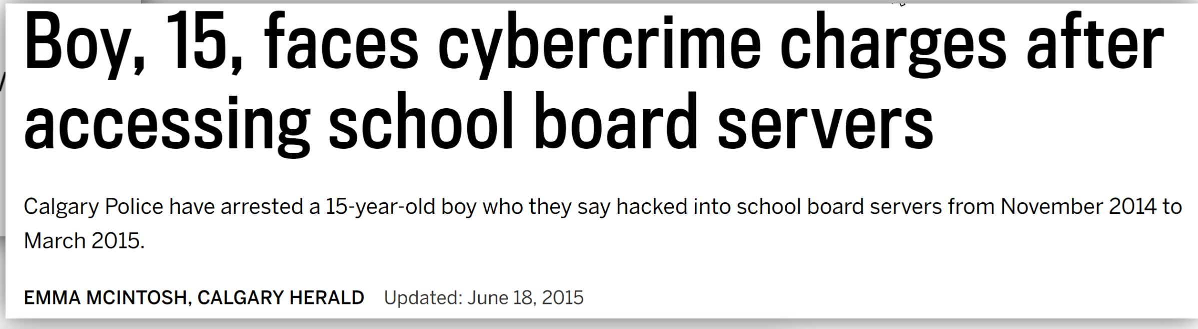
The Threat Landscape



Privacy breaches hit record high in Alberta

Privacy commissioner says more personal info online, hacking grow
sophistication

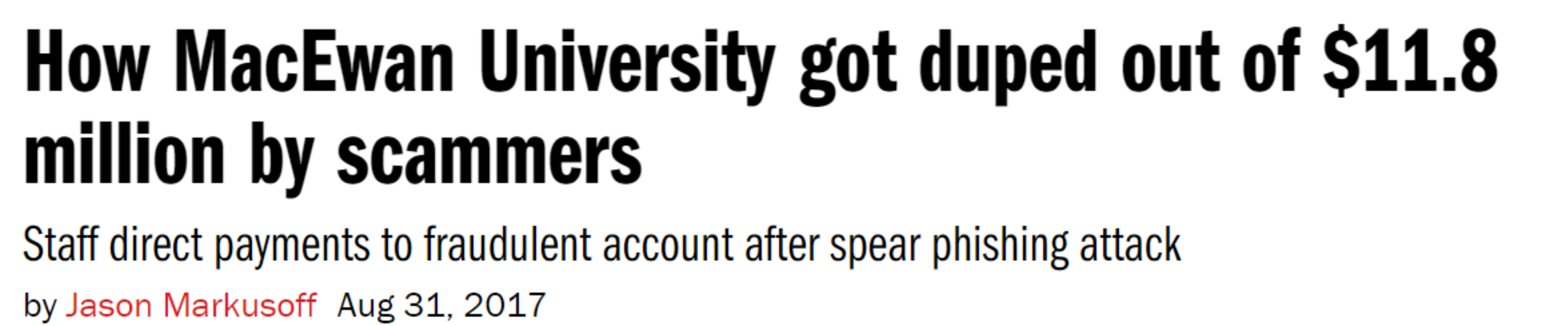
Scott Dippel · CBC News · Posted: Jan 06, 2018 6:00 AM MT | Last Updated: January 6



Boy, 15, faces cybercrime charges after accessing school board servers

Calgary Police have arrested a 15-year-old boy who they say hacked into school board servers from November 2014 to March 2015.

EMMA MCINTOSH, CALGARY HERALD Updated: June 18, 2015

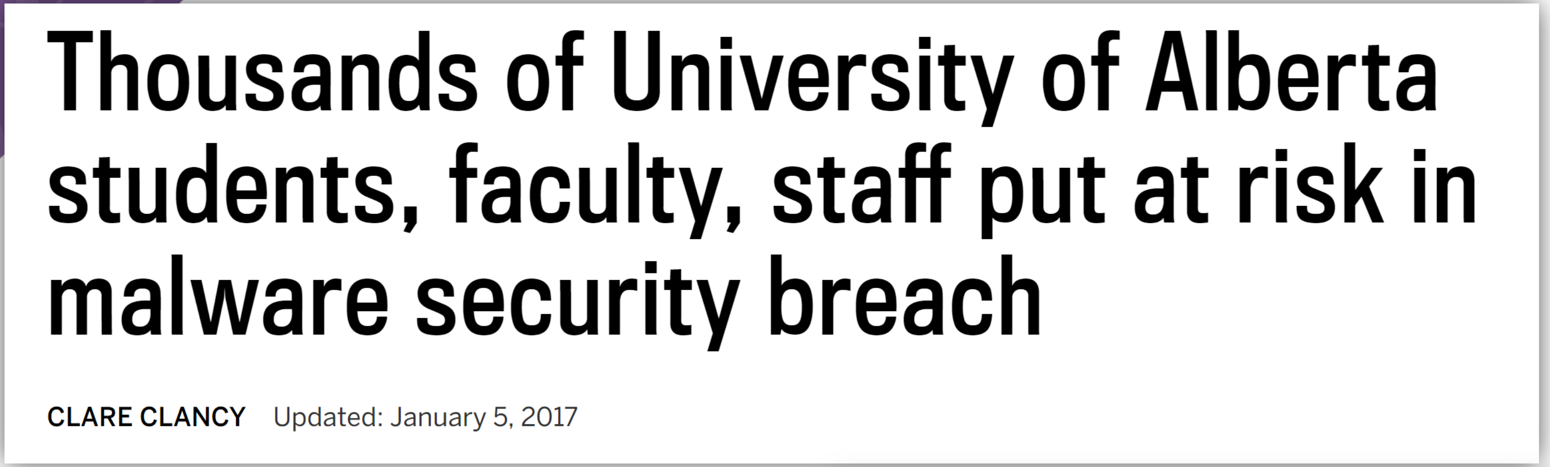


How MacEwan University got duped out of $11.8 million by scammers

Staff direct payments to fraudulent account after spear phishing attack

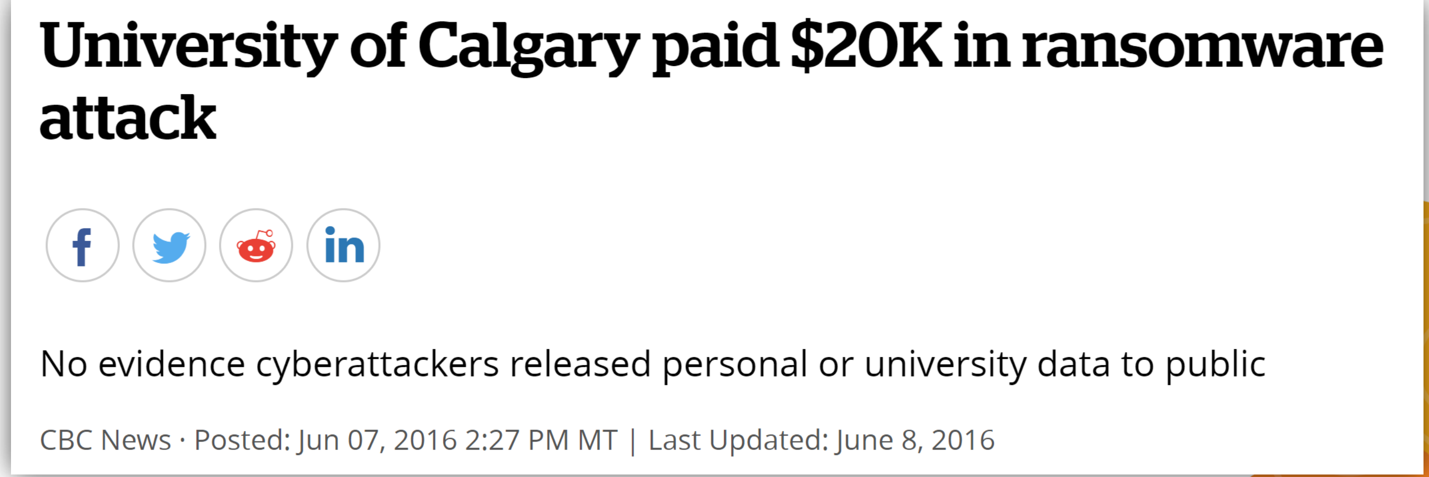
by Jason Markusoff Aug 31, 2017

The Threat Landscape



Thousands of University of Alberta students, faculty, staff put at risk in malware security breach

CLARE CLANCY Updated: January 5, 2017

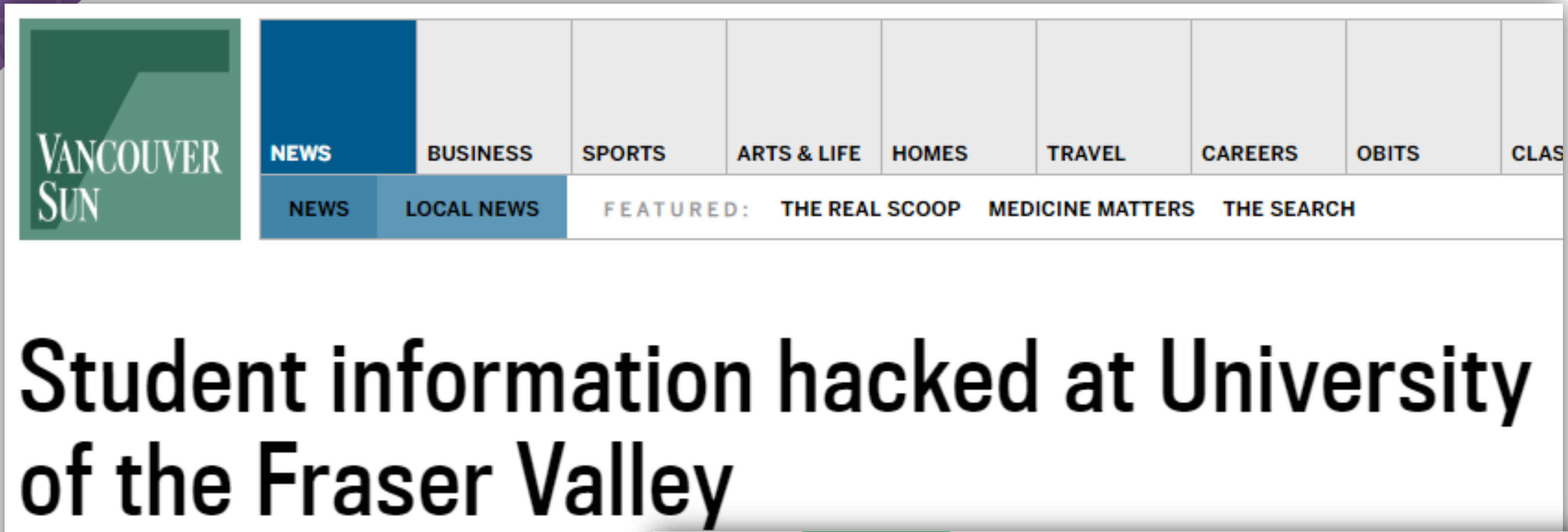


University of Calgary paid $20K in ransomware attack

No evidence cyberattackers released personal or university data to public

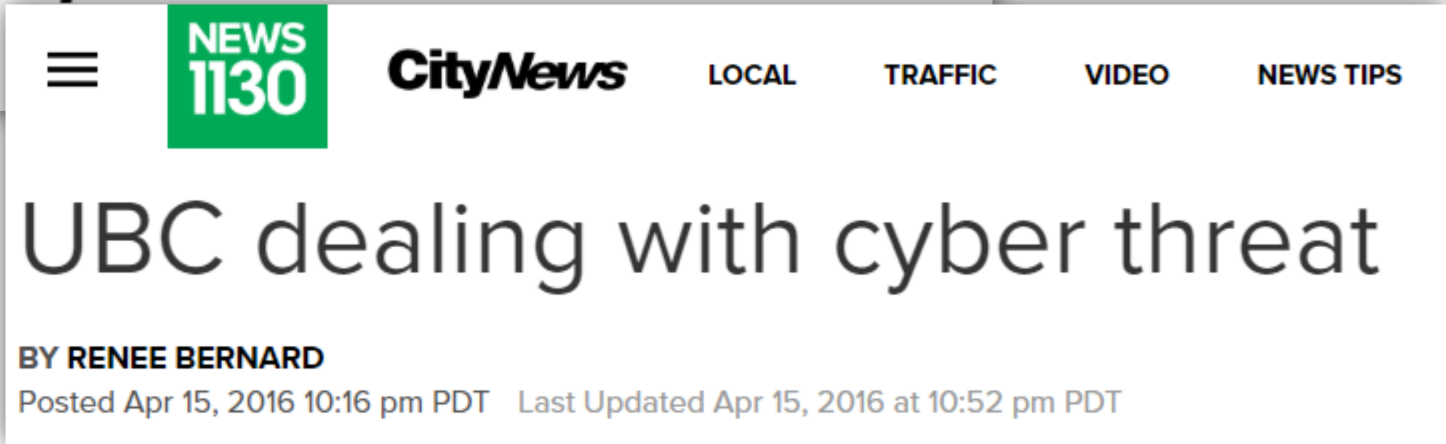
CBC News · Posted: Jun 07, 2016 2:27 PM MT | Last Updated: June 8, 2016

The Threat Landscape



Student information hacked at University of the Fraser Valley

JENNIFER SALTMAN Updated: November 1, 2017



UBC dealing with cyber threat

BY RENEE BERNARD

Posted Apr 15, 2016 10:16 pm PDT Last Updated Apr 15, 2016 at 10:52 pm PDT

Incidents are widespread

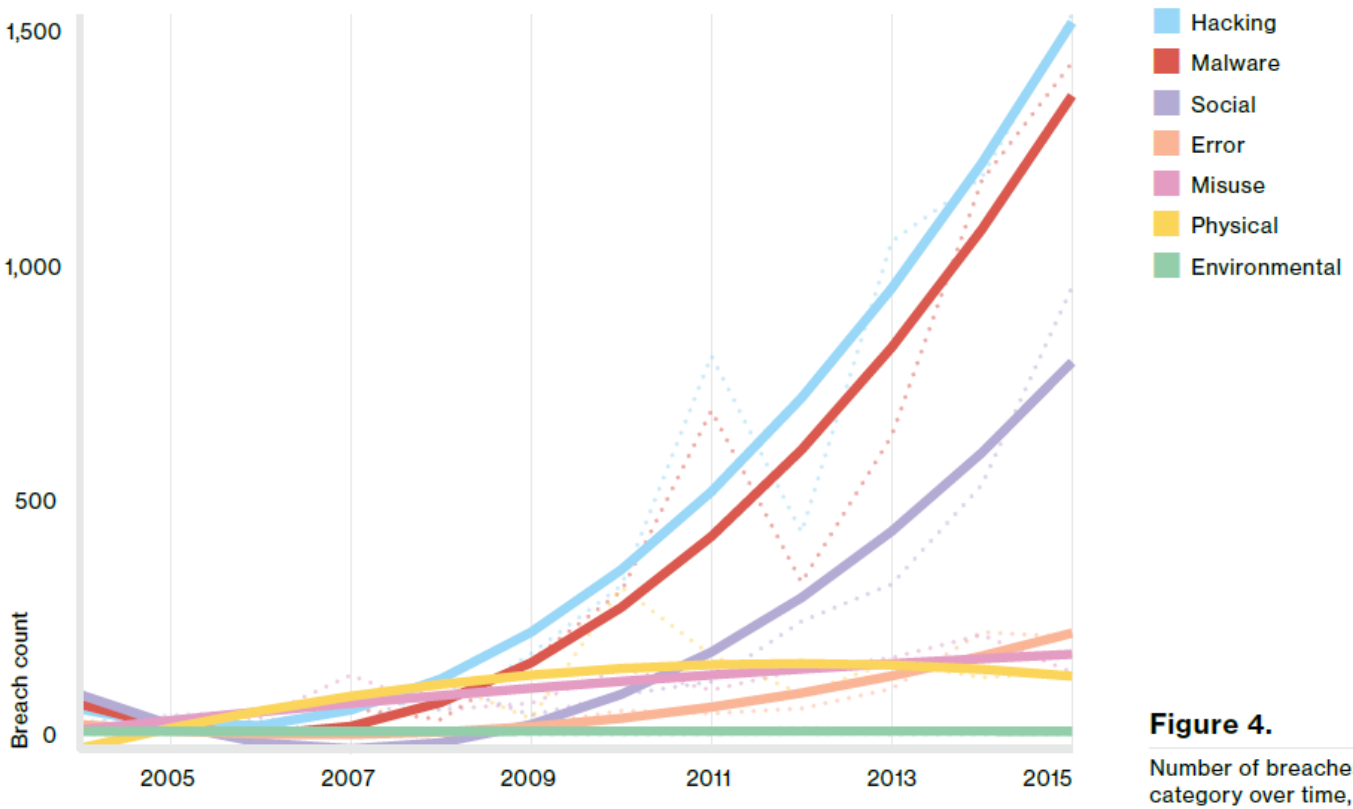
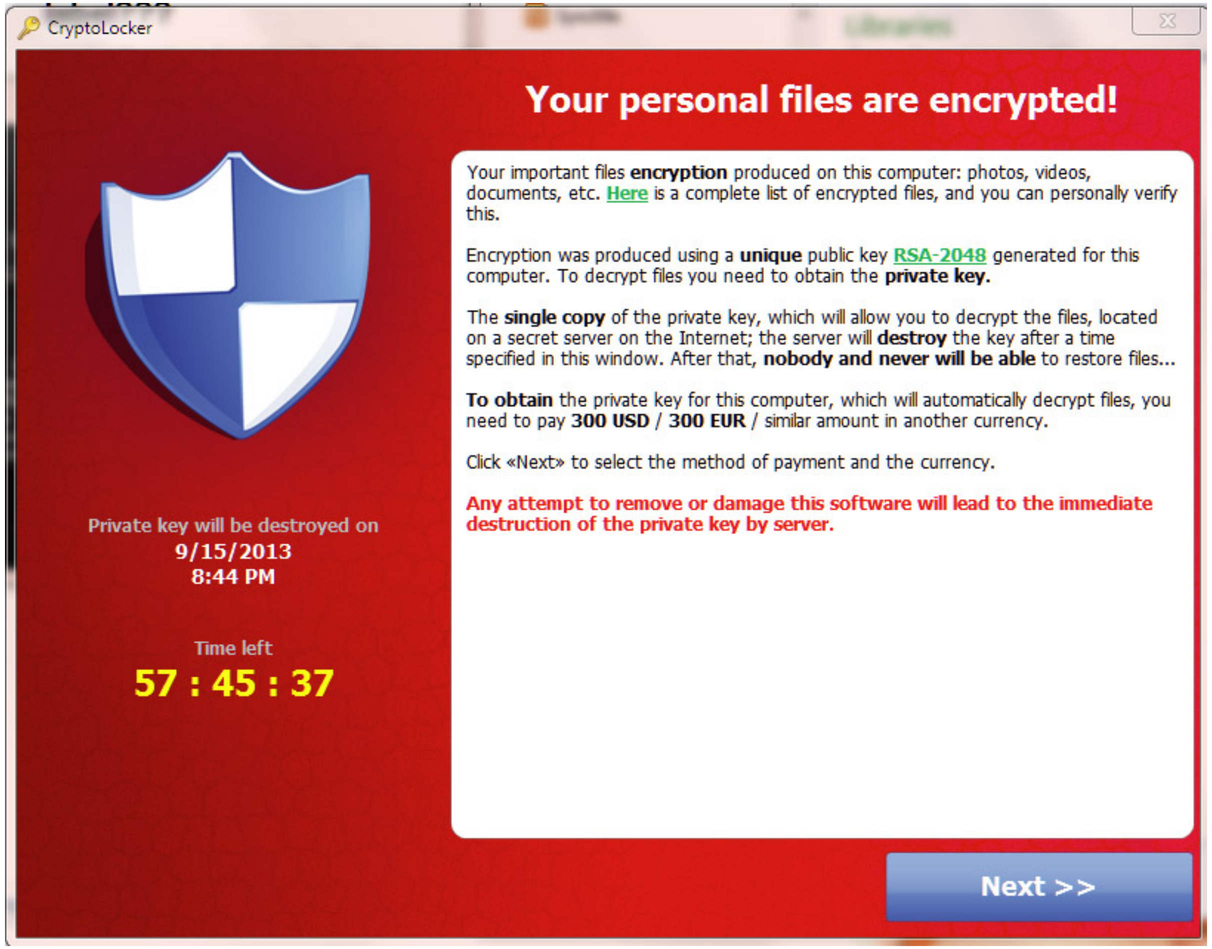


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

Ransomware



Your personal files are encrypted!

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 files you 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 **300 USD** / **300 EUR** / similar amount in another currency.

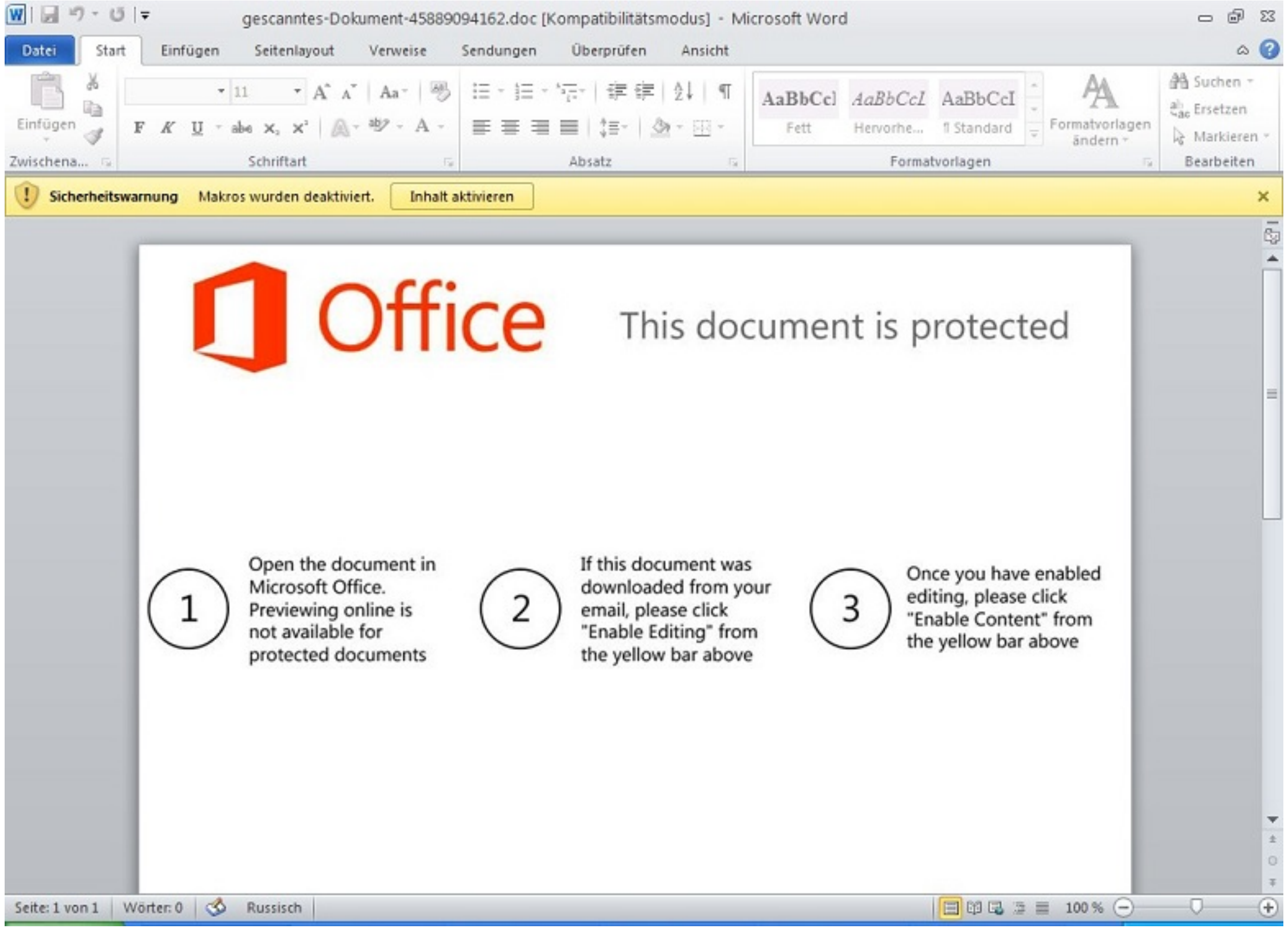
Click «Next» to select the method of payment and the currency.

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

Private key will be destroyed on
9/15/2013
8:44 PM

Time left
57 : 45 : 37

Malware embedded in Office Docs



gescanntes-Dokument-45889094162.doc [Kompatibilitätsmodus] - Microsoft Word

Sicherheitswarnung Makros wurden deaktiviert. Inhalt aktivieren

Office

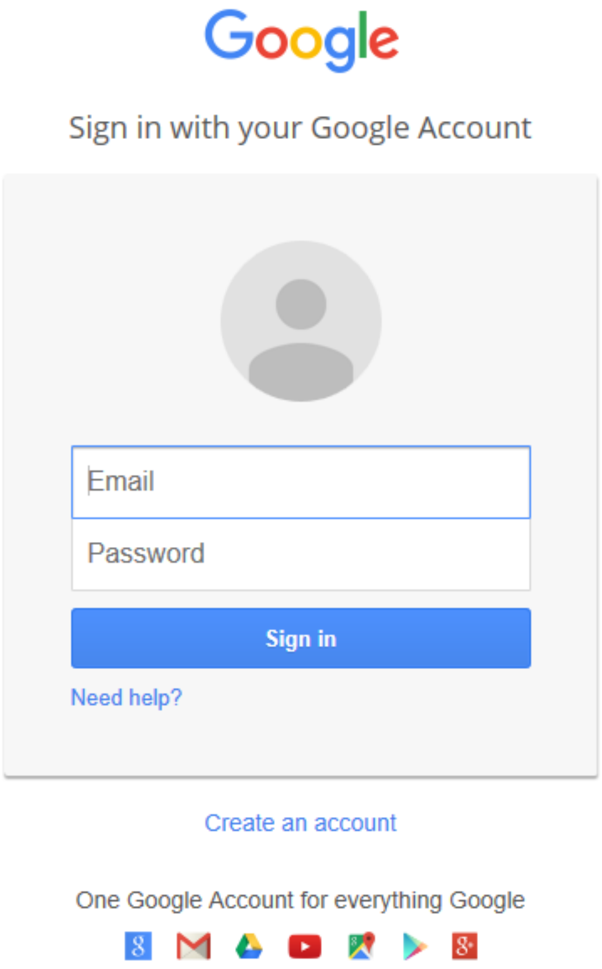
This document is protected

1 Open the document in Microsoft Office. Previewing online is not available for protected documents

2 If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above

3 Once you have enabled editing, please click "Enable Content" from the yellow bar above

Phishing

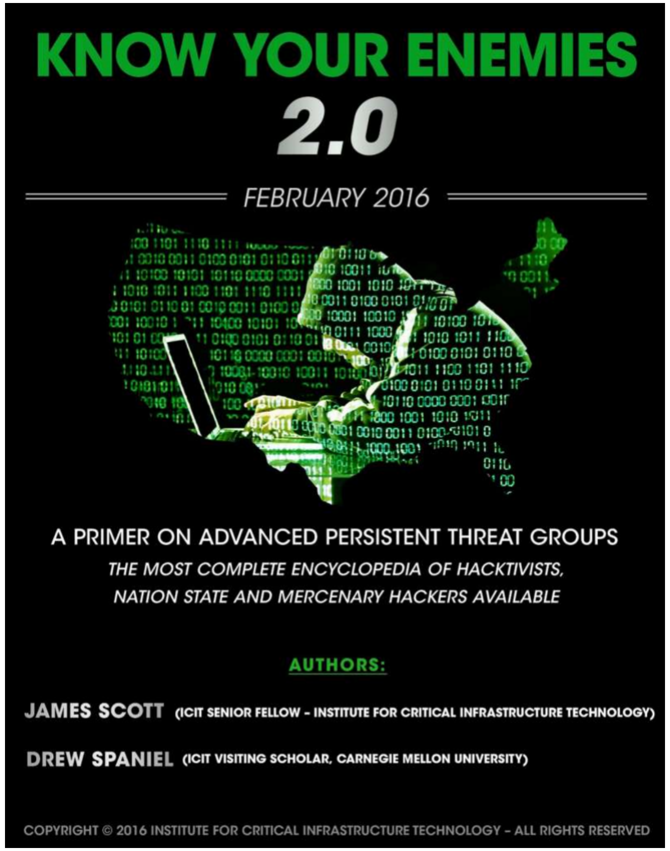


Sign in with your Google Account

One Google Account for everything Google

Advanced Threats are *Common*

- *Ajax/FLYINGKITTEN/Saffron Rose,america, Animal Farm, Anonymous, APT, APT 28/Sofacy Group/Sednit Group/Tsar Team/Fancy Bear/Operation Pawnstorm, APT29/Hammertoss/HammerDuke, Axiom, Blue Termite/Cloudy Omega/Emdivi, breach, Bureau 121/Guardians of Peace/Dark Seoul, Butterfly Group/orpho, Carbanak, China, CloudDuke/MiniDionis/CloudLook, CosmicDuke/Tinybaron/BotgenStudios/NemesisGemina. MiniDuke,CozyDuke/CozyCar/CozyBear/Office Monkeys/Cozer/EuroAPT, Dark Hotel/Tapaoux/Nemim/Pioneer/Karba, Deep Panda/Black Vine/ Pupa, Duqu/DQ, Elderwood Platform, Energetic Bear/Dragonfly/Havex Crouching Yeti/KoalaTeam28/Uroburos/EpicTurla/Snake/SnakeNet, EQUATIONGroup, Flame/Flamer/Skywiper, france, GeminiDuke, Hellsing, Hidden Lynx, Hidden Lynx/Aurora, Iran, Mirage, Moker, Naikon/APT 30, North Korea, OnionDuke, PinchDuke,PLA Unit 61398/Comment Crew/APT1, Putter Panda/APT2/PLAUnit61486, Regin/Prax/WarriorPride, Russia, Sandworm/Quedagh/BlackEnergy, Santa APT, SeaDuke/SeaDaddy/SeaDask, Shrouded Crossbow, south korea, syria, Tailored Access Operations (TAO),Tarh Andishan/Operation Cleaver, The Elderwood Platform, The Syrian Electronic Army (SEA)*



KNOW YOUR ENEMIES 2.0

FEBRUARY 2016

A PRIMER ON ADVANCED PERSISTENT THREAT GROUPS

THE MOST COMPLETE ENCYCLOPEDIA OF HACKTIVISTS, NATION STATE AND MERCENARY HACKERS AVAILABLE

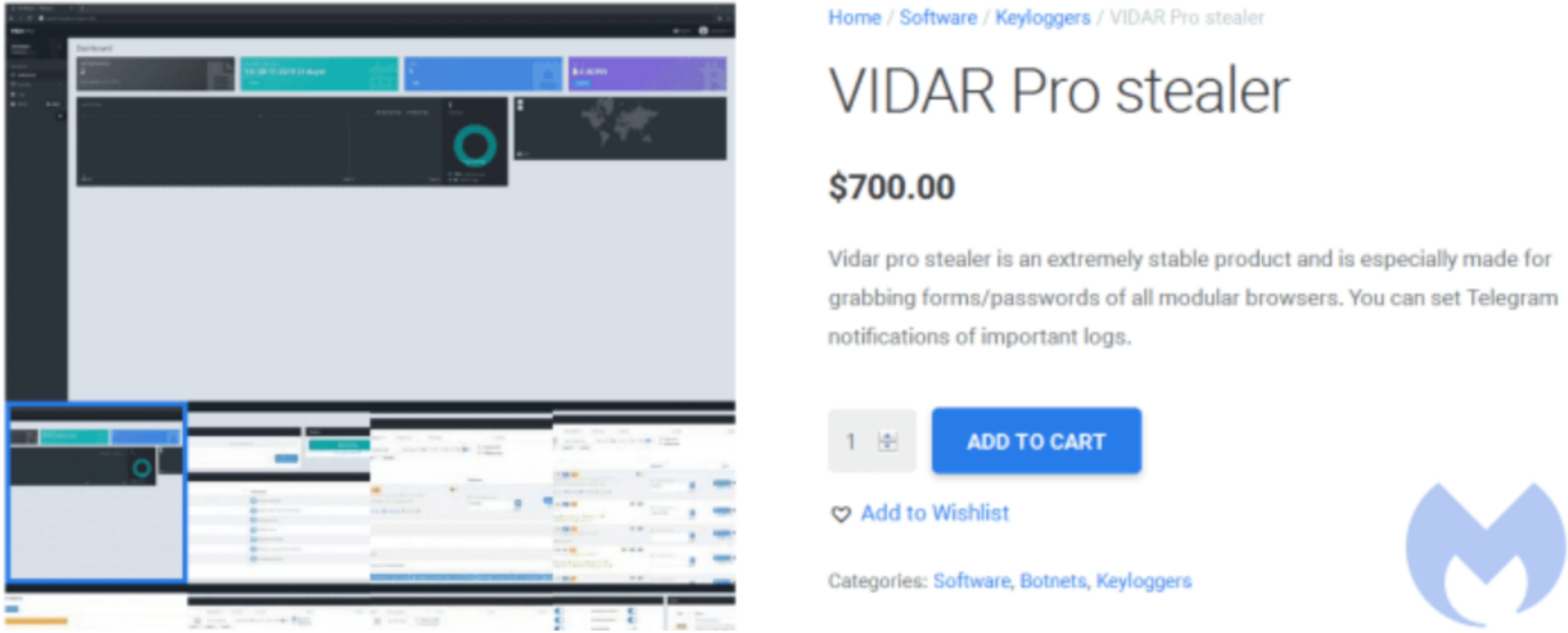
AUTHORS:

JAMES SCOTT (ICIT SENIOR FELLOW – INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY)

DREW SPANIEL (ICIT VISITING SCHOLAR, CARNEGIE MELLON UNIVERSITY)

COPYRIGHT © 2016 INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY – ALL RIGHTS RESERVED

Cybercrime Supply Chain



Home / Software / Keyloggers / VIDAR Pro stealer

VIDAR Pro stealer

$700.00

Vidar pro stealer is an extremely stable product and is especially made for grabbing forms/passwords of all modular browsers. You can set Telegram notifications of important logs.

Categories: Software, Botnets, Keyloggers

Credits : Malware Bytes

“Only as strong as your weakest link”

Vulnerabilities

1. Software bugs
2. Misconfigurations
3. Weak Processes
4. “People are too nice”
5. Passwords
6. Logic Errors

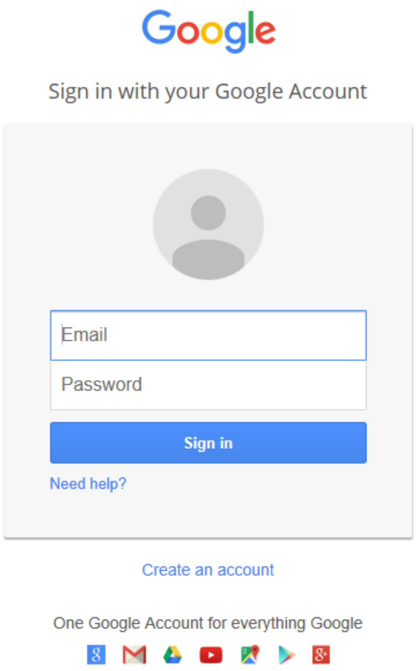
Demonstrations

Drive by Downloads

Demonstrations

Evading Antivirus

Cloning a Website and Phishing



Google

Sign in with your Google Account

Email

Password

Sign in

Need help?

Create an account

One Google Account for everything Google

“Only as strong as your weakest link”

But what happens when…

All the links are weak

The Gap between Threat and Defense

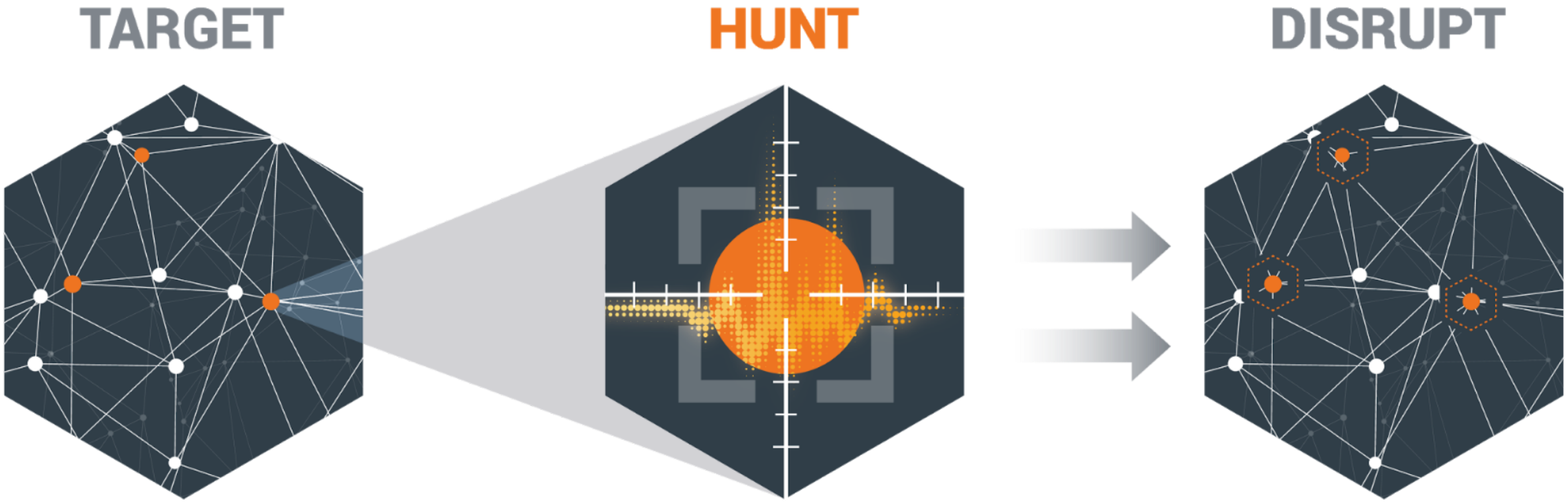
Attackers

- - Low cost to attack
- - Low cost to discover vulnerabilities
- - Low chance of being caught
- - Moderate chance of success
- - Moderate access to markets
- - Healthy supply chain
- - Short time between attack and reward

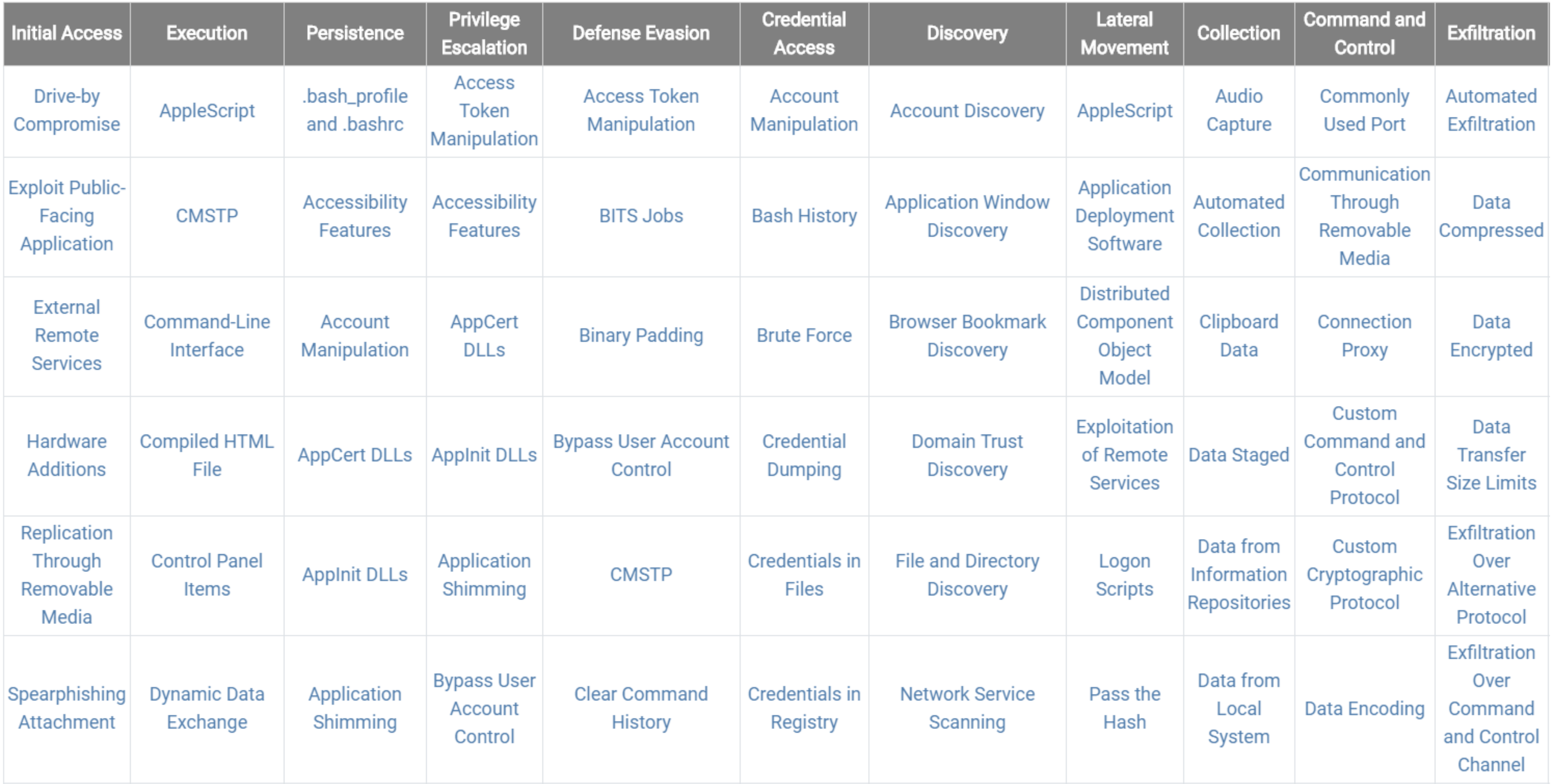
Defenders

- - High cost to defend
- - High cost to mitigate vulnerabilities
- - Low chance of detecting attacks
- - High cost of incident response
- - Excellent access to markets
- - Unhealthy supply chain
- - Long time between detection and recovery

From Threat Hunting to Disruption



MITRE ATT&CK



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel

BCNET 2019

Questions?

michael.mcdonnell@vcura.com