Chasing Foxes by the Numbers: Patterns of Life and Activity in Hacker Forums

Christopher Ahlberg, Co-Founder & CEO
Recorded Future
c@recordedfuture.com
@cahlberg
Attribution [Often] Based on Sloppy Handle Usage

UglyGorilla
SuperHard

GreenSky27

QQ identity
5054-3533

cpyy
Handles and Forums key to attribution

"CPYY"
Several email addresses have been associated with CPYY, who also appears to use the alternate handles CPYY and CPYY Chen.
- cpyy@fans.com
- cpyy@hotmail.com
- cpyychen@gmail.com
- cpyytiany.com

The cpyy.net domain lists "Chen Ping" as the registrant name, which may be CPYY's real name, as the characters with the initial "cp" in "cpyy".

The profile on the blog (shown in Figure 2) below indicates that the user is male, was born on 26 May 1979, and was at the "nano/ploy" site (~1998).
If Better Actor Opsec, Then What?

Forum Targeting

Key handles in forums

Handle hopping within and Across forums

Crews of handles

Can we apply some $R = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\left[\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2\right]^{1/2}}$?
Automated collection
750 hacker/criminal forums from Deep/Dark web
4 year collection
7 languages
Indexed
NLP/Feature extraction for cyber attacks, vulnerabilities, exploits, technical indicators, etc.
Surprisingly little handle re-use
96.6%+ used once
1,446,815 total
First Pattern: Hackers Have Hours

The Daily Rhythm of Crime in Chicago

- 6am
- noon
- 6pm

All Crimes
They Just Differ
Distinct Patterns
Multiple Geos or Crews?
Distinct Weekly Patterns

- All
- Iranian forum
Smoking out the Rats with External Events
Patch Tuesday Driving Exploit Wednesday
Patch Tuesday Drives Russian and Iranians
Even When Work Hours Are Different
Two Kings of Vulnerabilities
Clustering Pattern of Life
Understanding Behavior by Math

The correlation between two points, \( a \) and \( b \), with \( k \) dimensions is calculated as:

\[
\frac{\text{cov}(a, b)}{\text{std}(a) \times \text{std}(b)}
\]

where

\[
\text{cov}(a, b) = \frac{1}{k} \sum_{j=1}^{k} (a_j - \bar{a}) \times (b_j - \bar{b})
\]

\[
\text{std}(a) = \sqrt{\frac{1}{k} \sum_{j=1}^{k} (a_j - \bar{a})^2}
\]

\[
\bar{a} = \frac{1}{k} \sum_{j=1}^{k} a_j
\]

This correlation is called Pearson Product Momentum Correlation, simply referred to as Pearson's correlation or Pearson's \( r \). It ranges from \(-1\) to \(1\) where \(1\) is the highest correlation. Complete opposite points have correlation \(-1\).

- \(a\) and \(b\) are identical, which means they have maximum correlation.

- \(a\) and \(b\) are perfectly mirrored, which means they have the maximum negative correlation.
Sample: Hamada Bader (non malicious, selling IT products)
First Cut: HASSAN20 = CRISIS?
Clustering Pattern of Life
Identifying Hang Aroun ds
Identifying User Pods

- Exploit Target Category:
  - Android Exploit Targets
  - Malware (3)
    - AndroidRAT
    - DroidJack
  - Malware Category (1)
    - Remote Access Trojan...

- Attack Vector (5):
  - Browser Targeted Code Execution
  - Cross site scripting
  - Abuse of Application... Privilege Escalation
  - Cross site Request For...

CVE-2014-0160 (Heart...)
CVE-2014-6271 (Shellsh...
CVE-2014-3567 (POOD...)
CVE-2014-4114 (Band...)
MS14-058
CVE-2014-6515
MS14-056
MS14-060
MS14-066
CVE-2014-4113
Making the Wednesday Night .Onion Rounds
Making the Wednesday Night .Onion Rounds
Profiling the Store Admin

L-U: Welcome to our private store

We are LONDON-UNDERGROUND, and we are proud to welcome you to our private vendor store. We are here to cater to all your Cocaine needs.

We provide a fast, simple, safe way for customers across Europe to purchase high quality Cocaine using Bitcoin as a payment method.

We have 3 different product lines, so whether you are looking for an absolute bargain, or the absolute best Cocaine you can find, we will have a product for you.

Our 3 Cocaine product lines are as follows:
- Pure Columbian Fishscale Cocaine (95%) £70 a gram. This is a completely untouched product.
- Columbian MK1 (50%) £35 a gram
- Columbian MK2 (90%) £20 a gram

The MK1/MK2 product lines are a mix of Columbian Fishscale, and high quality Benzoceaine, for a
Profiling the Store Admin
Profiling the Store Admin

- Mention on Dec 16, 2015
  1+ reference • [Redacted] Market Forum
  I sell oxy and more.

- Mention on Dec 13, 2015
  1+ reference • [Redacted] Market Forum
  I bought cocaine and MDM from him several times.

- Mention on Nov 29, 2015
  1+ reference • [Redacted] Market Forum
  Using MG to buy drugs is the best way to get to jail...
Summary and What’s Next?

• Pattern of life on metadata supports attribution
• Lead generation [duh!] requiring secondary sourcing

• Build hard analytic: “find handles like this”
• Cross validation on secondary data sources

• Christopher Ahlberg, Co-Founder & CEO
• Recorded Future
• c@recordedfuture.com @cahlberg