Cybersecurity Big Data Research for Hacker Community: A Topic and Language Modeling Approach

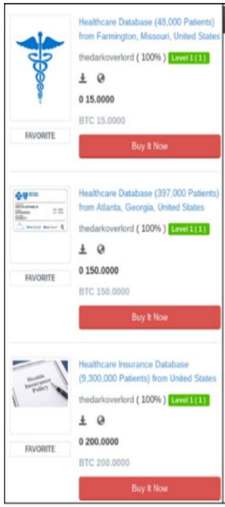
PI: Dr. Hsinchun Chen, University of Arizona; Co-PI: Dr. Weifeng Li, University of Georgia

Challenges:

- The technical difficulties in hacker community collection
- The massive volume of the data
- The heterogeneity and covert nature of the data elements and their subtle linkages
- The need to comprehend subcultural nature of terms and concepts embedded in the hacking community across multiple foreign languages

Solution:

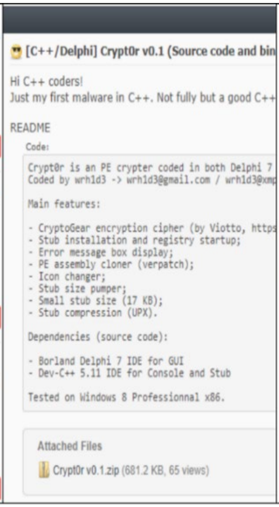
- A large and comprehensive testbed of significant international online hacker communities
- An *adversarial deep representation* approach to learning the language-invariant representations from content in English and non-English hacker communities
- A *nonparametric supervised topic modeling* method for examining customer reviews of hacker assets
- A *scalable dynamic topic modeling* technique designed for incorporating expert knowledge of hacker communities



Healthcare Database (48,000 Patients) from Farmington, Missouri, United States
thedarkoverlord (100%) Level 1 (1)
0 15.0000
BTC 15.0000

Healthcare Database (397,000 Patients) from Atlanta, Georgia, United States
thedarkoverlord (100%) Level 1 (1)
0 150.0000
BTC 150.0000

Healthcare Insurance Database (9,300,000 Patients) from United States
thedarkoverlord (100%) Level 1 (1)
0 200.0000
BTC 200.0000



[C++/Delphi] Crypt0r v0.1 (Source code and bin

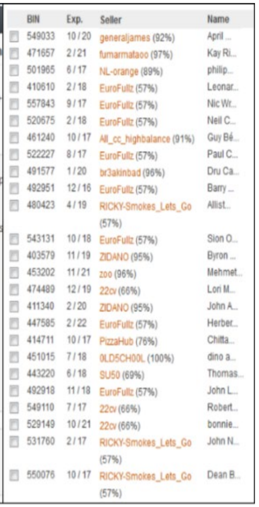
Hi C++ coders!
Just my first malware in C++. Not fully but a good C++

README

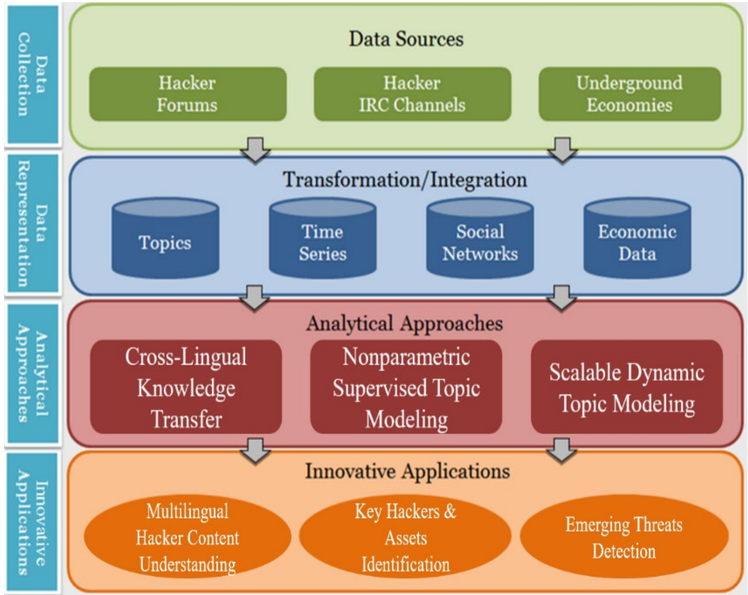
Code:

```
Crypt0r is an PE crypter coded in both Delphi 7
Coded by wrh1d3 -> wrh1d3@gmail.com / wrh1d3@xmp

Main features:

- CryptoGear encryption cipher (by Viotto, https
- Stub installation and registry startup;
- Error message box display;
- PE assembly cloner (verpatch);
- Icon changer;
- Stub size pumper;
- Small stub size (17 KB);
- Stub compression (UPX).

Dependencies (source code):

- Borland Delphi 7 IDE for GUI
- Dev-C++ 5.11 IDE for Console and Stub

Tested on Windows 8 Professionnal x86.
```

Attached Files
Crypt0r v0.1.zip (681.2 KB, 65 views)



	BIN	Exp.	Seller	Name
□	549033	10 / 20	generaljames (92%)	April ...
□	471657	2 / 21	fumarmataoo (97%)	Kay Ri...
□	501965	6 / 17	NL-orange (89%)	philip...
□	410610	2 / 18	EuroFullz (57%)	Leonar...
□	557843	9 / 17	EuroFullz (57%)	Nic Wr...
□	520675	2 / 18	EuroFullz (57%)	Neil C...
□	461240	10 / 17	All_cc_highbalance (91%)	Guy Bé...
□	522227	8 / 17	EuroFullz (57%)	Paul C...
□	491577	1 / 20	br3akinbad (96%)	Dru Ca...
□	492951	12 / 16	EuroFullz (57%)	Barry ...
□	480423	4 / 19	RICKY-Smokes_Lets_Go (57%)	Allist...
□	543131	10 / 18	EuroFullz (57%)	Sion O...
□	403579	11 / 19	ZIDANO (95%)	Byron ...
□	453202	11 / 21	zoo (96%)	Mehmet...
□	474489	12 / 19	22cv (66%)	Lori M...
□	411340	2 / 20	ZIDANO (95%)	John A...
□	447585	2 / 22	EuroFullz (57%)	Herber...
□	414711	10 / 17	PizzaHub (76%)	Chilta...
□	451015	7 / 18	0LD5CH00L (100%)	dino a...
□	443220	6 / 18	SU50 (69%)	Thomas...
□	492918	11 / 18	EuroFullz (57%)	John L...
□	549110	7 / 17	22cv (66%)	Robert...
□	529149	10 / 21	22cv (66%)	bonnie...
□	531760	2 / 17	RICKY-Smokes_Lets_Go (57%)	John N...
□	550076	10 / 17	RICKY-Smokes_Lets_Go (57%)	Dean B...



Scientific Impact:

- Understanding the human behaviors behind malicious online acts such as cybercrime and cyberterrorism is an important objective in gaining a better understanding of the cyber threat landscape.
- Hacker communities are of particular interest as they allow hackers to share malicious assets such as hacking tools, malware source code, and hacking tutorials with one another.

Broader Impact:

- Benefiting several stakeholder communities: Intelligence and Security Informatics (ISI), NSF Scholarship-for-Service (SFS), National Cyber-Forensics & Training Alliance (NCFTA), and The Society for the Policing of Cyberspace (POLCYB).
- Integration into education: AZSecure SFS, NSA designated Center of Academic Education in Cyber Defense (CAE-CD) courses at UA, UA's online MS in Cybersecurity program, UGA's undergraduate area of emphasis in Information Security

NSF Award#1936370

PI: Dr. Hsinchun Chen (hsinchun@email.arizona.edu)
Co-PI: Dr. Weifeng Li (weifeng.li@uga.edu)