Cybersecurity initiatives at the University of Ottawa

November 28 2022

uOttawa is making cybersecurity and cybersafety a priority

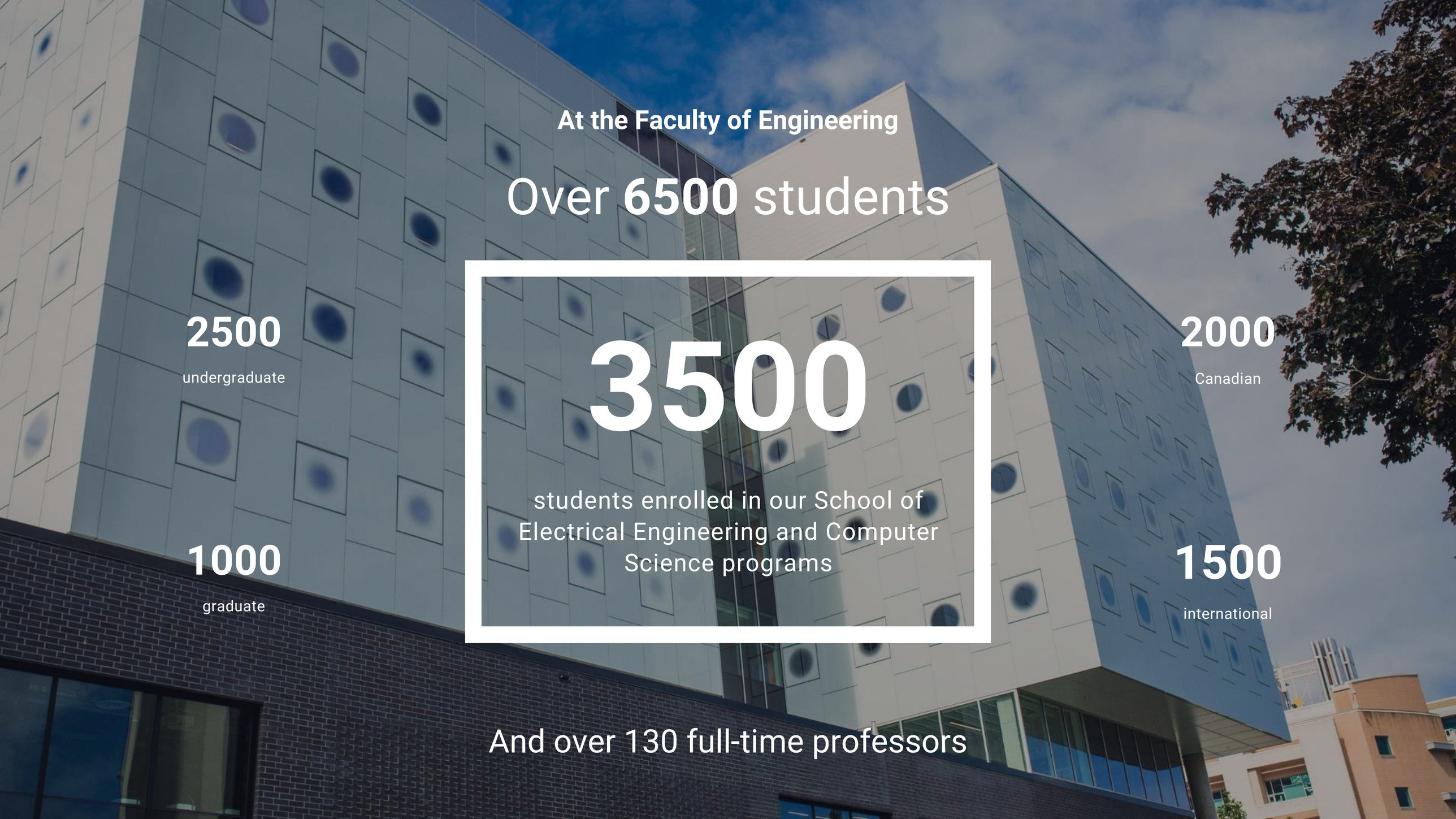
We are tackling the growing threat of cyber attacks and cyber crime head on.

CYBER
carrefour • hub

The Cyber Hub is designed to be:

- Inclusive
- Interdisciplinary
- Integrated
- Immersive
- Innovative

Brings together world-class researchers, experts and leaders to drive excellence in experiential training and interdisciplinary research in cybersecurity and cybersafety.



At the Faculty of Engineering

Over **6500** students

2500

undergraduate

1000

graduate

3500

students enrolled in our School of Electrical Engineering and Computer Science programs

2000

Canadian

1500

international

And over 130 full-time professors

The uOttawa-IBM Cyber Range

Enabling learning, training, research, and outreach

About the Cyber Range

Located in the Cyber Hub, the Cyber Range, created in partnership with IBM, will deliver security training, professional development, and partnering opportunities in both official languages to help grow Canada’s skilled cybersecurity and cybersafety workforce across government, academia and industry.

Our Cyber Range directors

Guy-Vincent Jourdan

Professor
Faculty of Engineering
University of Ottawa

Vio Onut

Principal R&D Strategist
Centre for Advanced Studies
IBM

About IBM Security

Leveraging IBM extended Security & Higher Education teams as needed

IBM **Security**

Security Operations

- 12 Global and Regional SOCs (Managing Clients SOC operations) monitoring 4.7 trillion events per month from 20,000-plus devices
- Entrusted by Clients for tactical Security Incident Response
- 50 years in security business

uOttawa × IBM

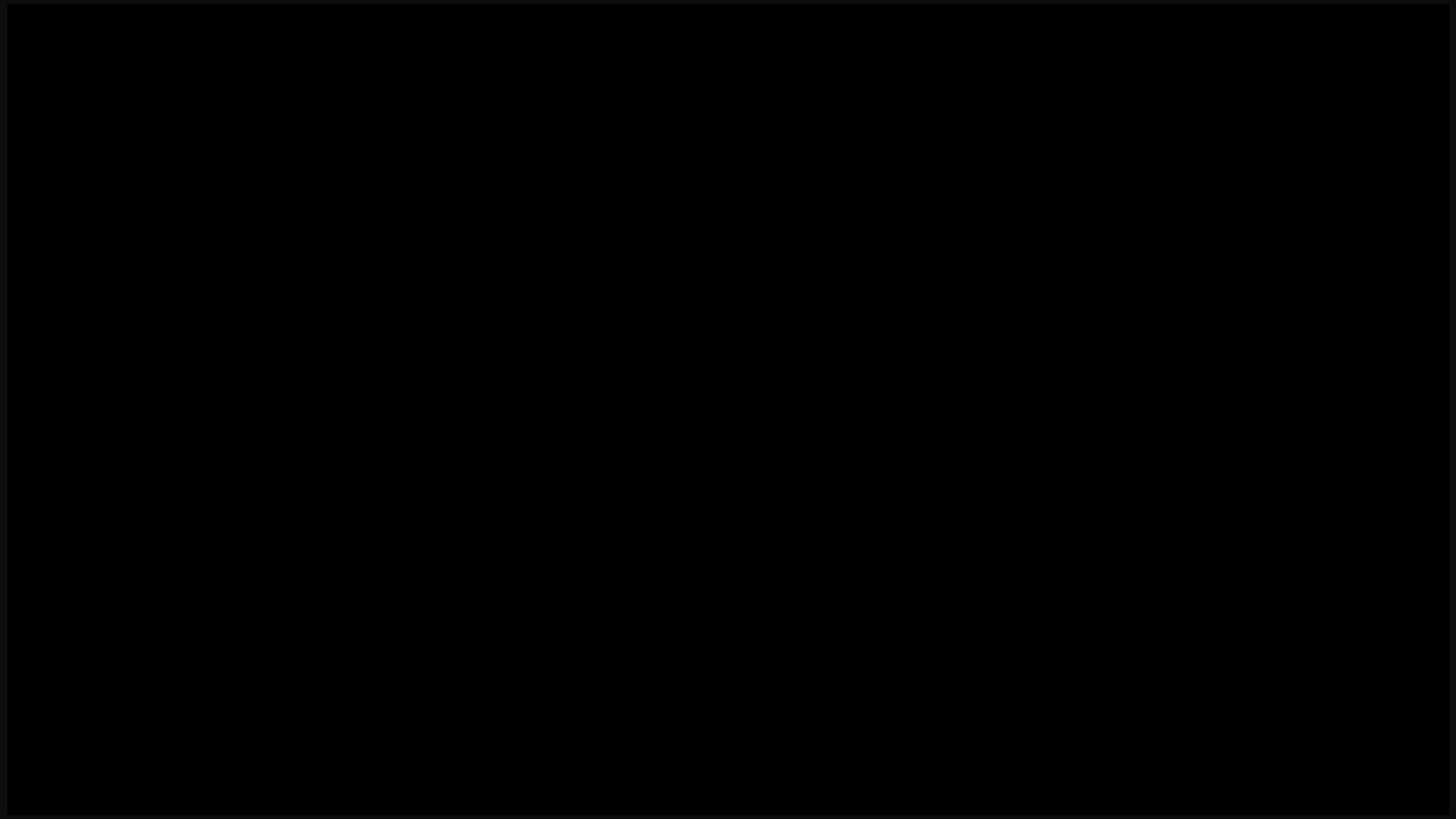
Training

- Our Cyber Ranges train 10,500+ clients
- industry's first cyber range for commercial, government, healthcare and academia
- a first-of-its-kind training, simulation and security operations center on wheels

Research

- Threat Prevention, Detection & Investigation
- Threat Response and Recovery
- Security Technology Management & Monitoring

IBM



https://youtu.be/WC6ABBhupYw

Floor Plan


IT ROOM
502
ELECT.
500W
CORRIDOR
500
OPEN TO BELOW
05
ELEVATORS
500X
ELEVATORS
500Y
SIMULATION RM #2
560
LOCKERS
501
CORRIDOR
RECEPTION
500
KITCHENETTE
504
BROADCASTING RM
505
OFFICE #1
512
OFFICE #2
511
ELEC
574
FORENSIC RM
506
HOTELING STATIONS
510
CORRIDOR
EXIT STAIR B
5B
QUIET RM
507
SERVER / RISER RM
502
SIMULATION RM #1
503
LIVE RANGE RM
509
COMMAND AND CONTROL RM
508
LOCKERS
501
CORRIDOR

Rendering of Main Cyber Range Room

Server Room

The Cyber Range is multi-year partnership with IBM to create a fully immersive, interactive, and experiential learning facility for research and training in cybersecurity for students, businesses, and government organizations.

IBM

uOttawa

Immersive Learning

Powered by state-of-the-art technology, integrated within our curriculum and in partnership with companies and government.

Tailored Training

Real-world scenarios, advanced simulations and an immersive delivery experience.

Interdisciplinary Research

Into new areas of threat defence, analytics, AI security, cyber law, and organizational response.

Community Building

Create the next generation of experts by engaging with youth, uniting the cyber community and by attracting a diverse talent pool.

ACADEMIC PROGRAMS

Cyber Range training will be integrated into undergraduate and graduate courses, and within microprograms.

PROFESSIONAL SKILLS DEVELOPMENT

New microprograms and micro-credentials are open to professionals, with flexible delivery and adapted schedule.

INDUSTRY CERTIFICATION

Cyber Range training will be coupled with industry certifications (NSE, IBM, CompTIA, and more).

Immersive Learning

Tailored Training

A unique cybersecurity training and testing facility that provides experiential learning opportunities that are both immersive and ultra-realistic.

TRAINING PLATFORM

Access the Cyber Range to upskill or reskill your team, and validate technical skills using our wide array of cybersecurity scenarios.

CYBERSECURITY RESPONSE

Immerse your technical and leadership teams in an engaging session to hone your cybersecurity response.

CUSTOMIZABLE ENVIRONMENT

Build an interactive emulation of your local network, systems, tools, and applications using the CITEF™

Interdisciplinary Research

Key National Cyber Research Infrastructure

Meet our Cyber Experts

Carlisle Adams

cadams@uOttawa.ca

Cryptography and Computer Security Research

Cryptography, network security, computer security, access control, and privacy.

Roland Bouffanais

rbouffan@uOttawa.ca

Secure Networked Systems

Control strategies for 5G+ networks enabling anticipated and reactive architectures and algorithms for security.

Paula Branco

pbranco@uOttawa.ca

AI Methods to Detect Fraud, Scams, and Intrusions

Malware detection, intrusion detection, network traffic anomaly detection, misuse and signature detection.

Meet our Cyber Experts

Lionel Briand

lbriand@uOttawa.ca

AI-Based Software Security Testing and Analysis

AI-based solutions for automated security testing and analysis of application software.

Guy-Vincent Jourdan

gjourdan@uOttawa.ca

Cryptography, Computer and Network Security, and Privacy Technologies

Distributed systems modelling and analysis, software security, cybercrime detection and prevention and ordered sets.

Paria Shirani

pshirani@uOttawa.ca

Cybersecurity of Firmware and IoT

Anomaly detection, cyber-persona identification, IoT security, malicious code, malware analysis, vulnerability detection.

Community Building

- Host events, conferences, seminars, and hackathons to bring together the cyber community.
- Support youth in their journey to build cybersecurity literacy with local outreach programs for kids and teens such as workshops, summer camps, enrichment programs, demos, and more.
- Build international collaborations with other educational institutions to expand the talent pool.
- Support historically underrepresented students with programming, scholarships, and grants to incentivize greater diversity in this field.

Partnership uOttawa and Fortinet

WHO IS FORTINET?

- Largest pure play cybersecurity company, with over 10,000 employees globally
- Headquartered in Sunnyvale, California
- 50+ products across 8 different solution areas
- Founded in 2000
- IPO 2009 ($156M > $54B) added to S&P 500 in 2018

THEIR CANADIAN PRESENCE

- Primary development office in Burnaby, BC
- FortiGuard Research Labs in Burnaby, BC
- Largest North American Support Centre in Ottawa
- Fortinet NSE Training Institute in Ottawa
- Approx. 1,800 Canadian employees

Fortinet has over 450 Partners around the globe, however they only have six Strategic Partners. uOttawa is the exclusive Canadian Strategic Partner.

Strategic Partnership

Custom training program to increase talent recruitment

- Integration of Fortinet training material into uOttawa courses and micro-credential
- Full access to cloud-based labs and certification vouchers for our students (NSE 4)
- Certified students given paid internship opportunities
- Secured a collaborative provincial grant for the development of a micro-credential course

Inside the Cyber Range

Integrating Fortinet offer into the Range

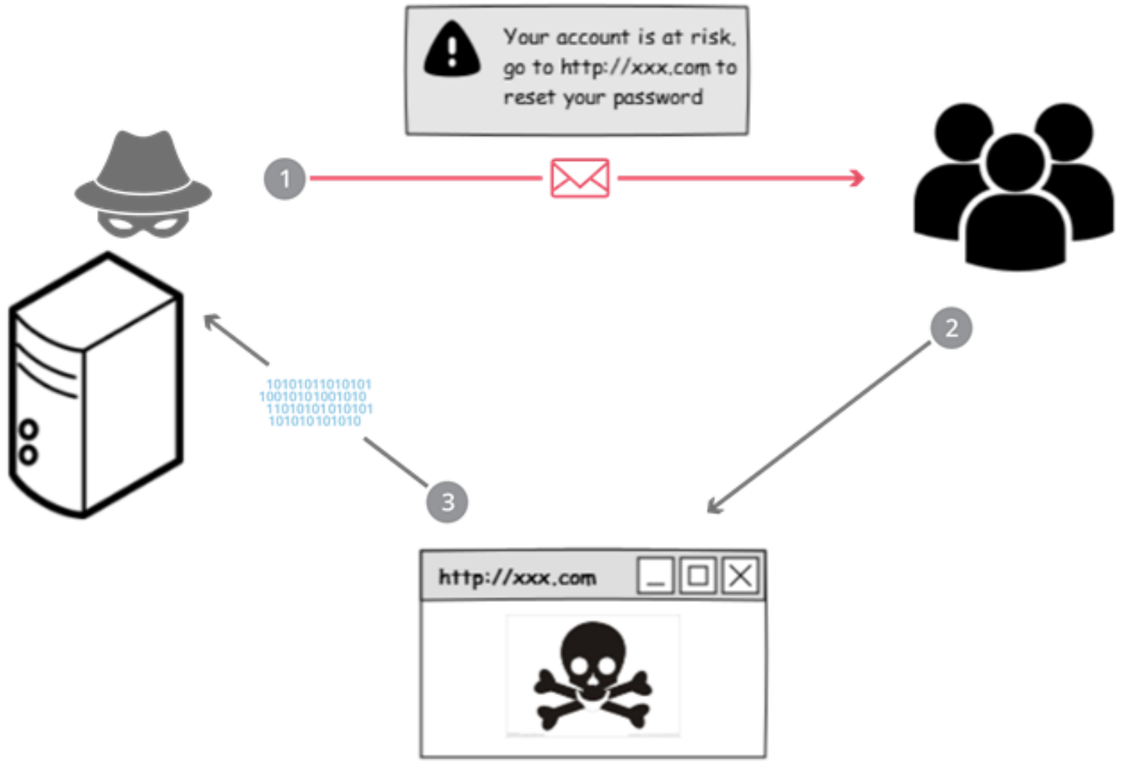
- Provided over $1M worth of VM and licenses to use in training and in research
- Once the range goes live, Fortinet will provide hardware, allowing hands-on experience for both trainees and grad students
- Working on a larger, federal grant involving Fortinet equipment supporting this state-of-the-art new facility

Research collaboration

Internationally trusted research and innovation

- Establishing key research projects between Fortinet’s R&D department and the research teams at uOttawa Engineering, in particular around AI and cybersecurity
- Fortinet is an industry partner for an infrastructure grant application for the Cyber Range research lab

Phishing attacks



internet attack impersonating trustworthy website

Tricks end-users into providing sensitive information

Phishing Attack Detection and Evolution (client side)

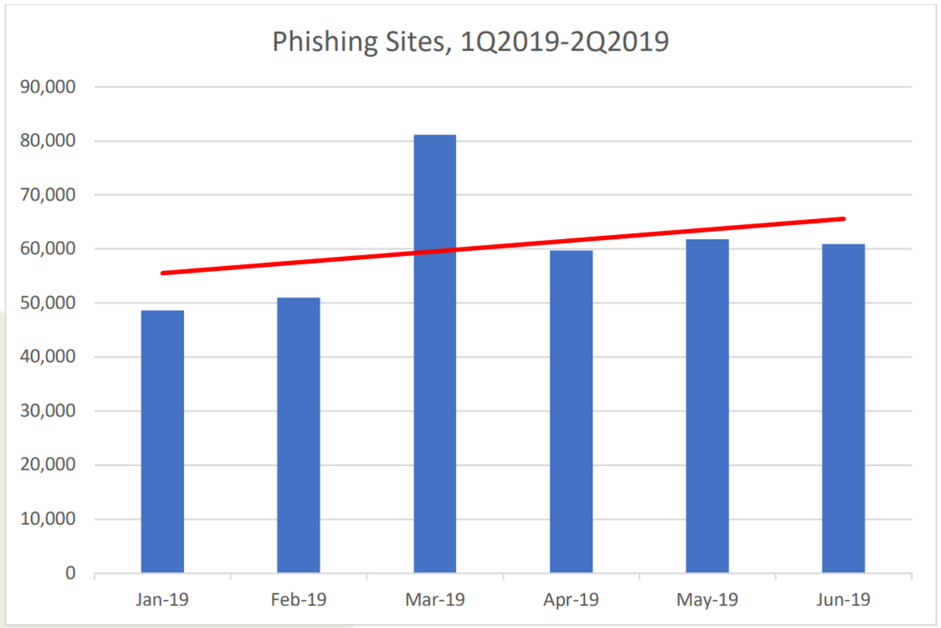
Cui, Q., Jourdan, G.-V., Bochmann, G. v., Onut, I.V and Flood, J. **Phishing Attacks Modications and Evolutions**, *Proceedings of ESORICS 2018, Barcelona, Spain, September 2018.*

LePage, S., Cui, Q., Jourdan, G.-V., Bochmann, G. v., Flood, J., and Onut, I.V. **Using AP-TED to Detect Phishing Attack Variations**, proceedings of the 16th conference on Privacy, Security and Trust (PST 2018), Belfast, Ireland, August 2018

Cui, Q., Jourdan, G.-V., Bochmann, G. v., Couturier, R., and Onut, I.V. **Tracking Phishing Attacks Over Time** , in *26th World Wide Web Conference (WWW'17), Perth, Australia, April 2017*

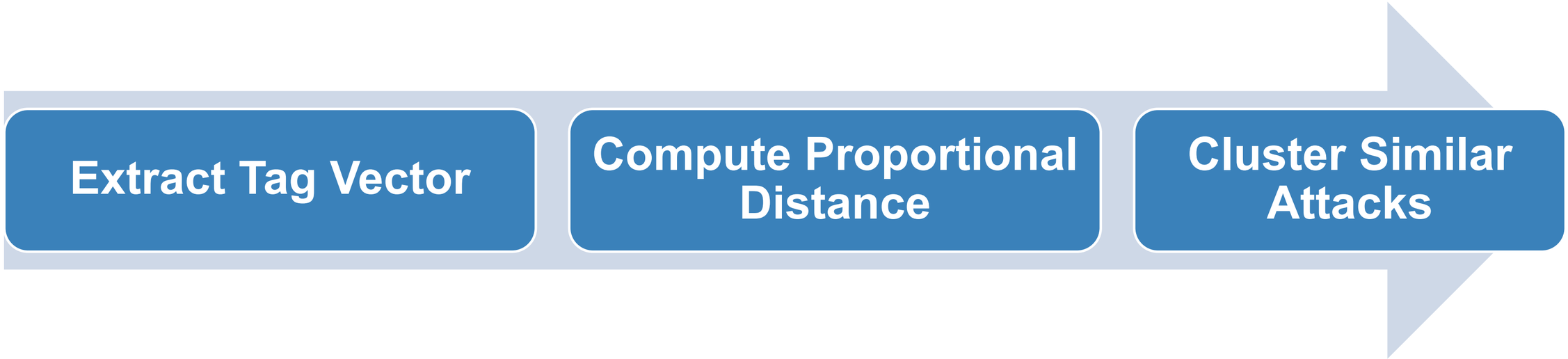
Phishing Attack Detection and Evolution (client side)

APWG 2019 Q1,Q2 report



- Lifespan of an attack is very short
- Attackers need to constantly renew attacks
- Building from scratch not economically viable
- Attacks are recycled
- Duplicate detection faster

Phishing Attack Detection and Evolution (client side)



TAG VECTOR = NUMBER OF TIMES EACH HTML TAG APPEARS IN THE DOM

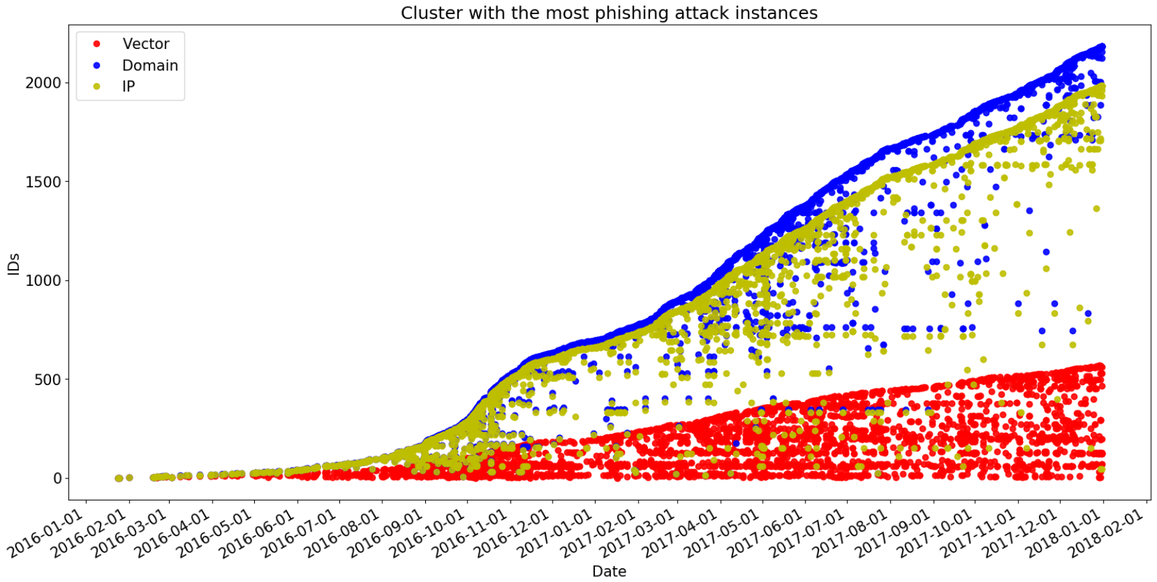
$$PD(T1, T2) = \frac{Hamming\ Distance}{\#\ of\ tags\ that\ appear\ in\ at\ least\ one\ vector}$$

DATABASE:~100K ATTACKS (PHISHTANK, IBM X-FORCE, OPENPHISH)

- DETECTION > 90%
- FALSE POSITIVE ~ 0.5%

Phishing Attack Detection and Evolution (client side)

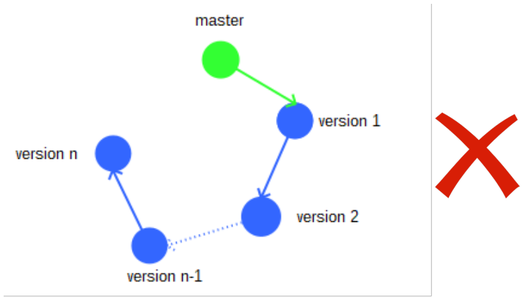
- More than 40% of the clusters are active for more than within one month
- Some remain live for two+ years, including more than 20% phishing instances.

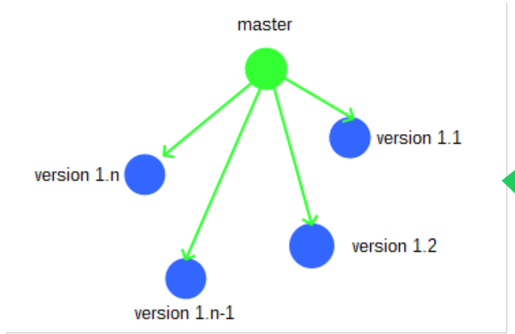


Phishing Attack Detection and Evolution (client side)

VARIATION HISTORY

Average length of variation path	**< 2**
Average update interval	**186 days**

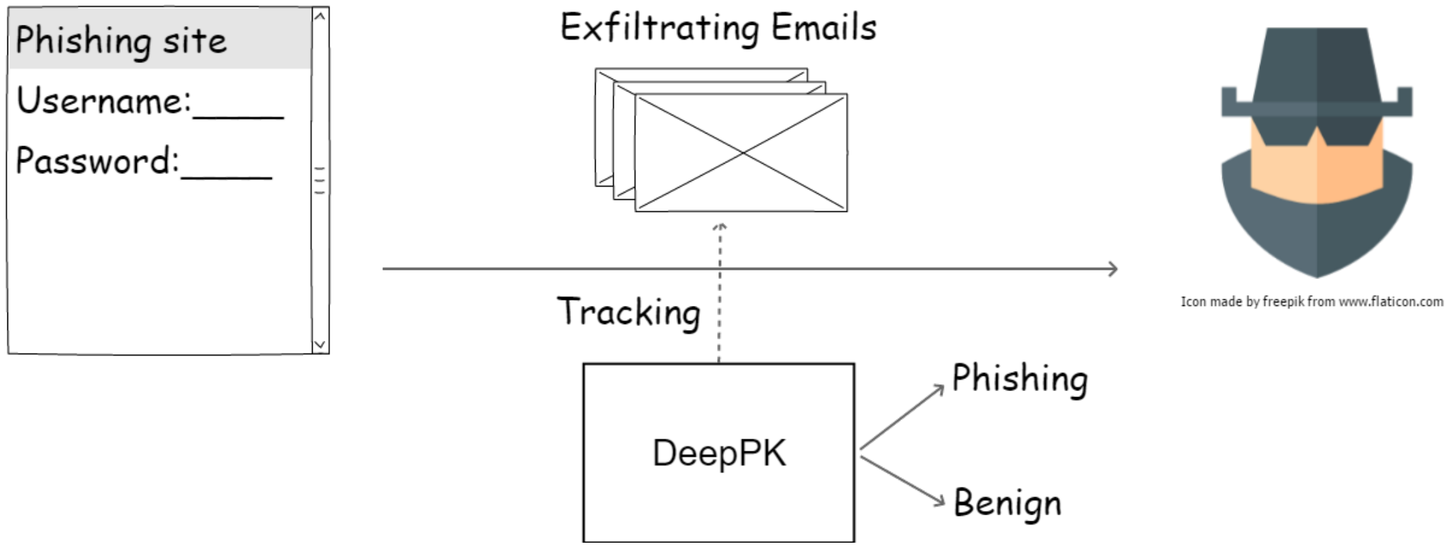




0-delay phishing attack detection using machine learning (server side)

Cui, Q., Jourdan, G.-V. and Onut, I.V, **Proactive Detection of Phishing Kit Traffic,** *19th International Conference on Applied Cryptography and Network Security, Kamakura, Japan, June 21-24, 2021*

0-delay phishing attack detection using machine learning (server side)



Detection of an attack being deployed on a network

- No active scan of the network
- No prior report requirement
- ZERO delay in detection => ZERO victim

0-delay phishing attack detection using machine learning (server side)

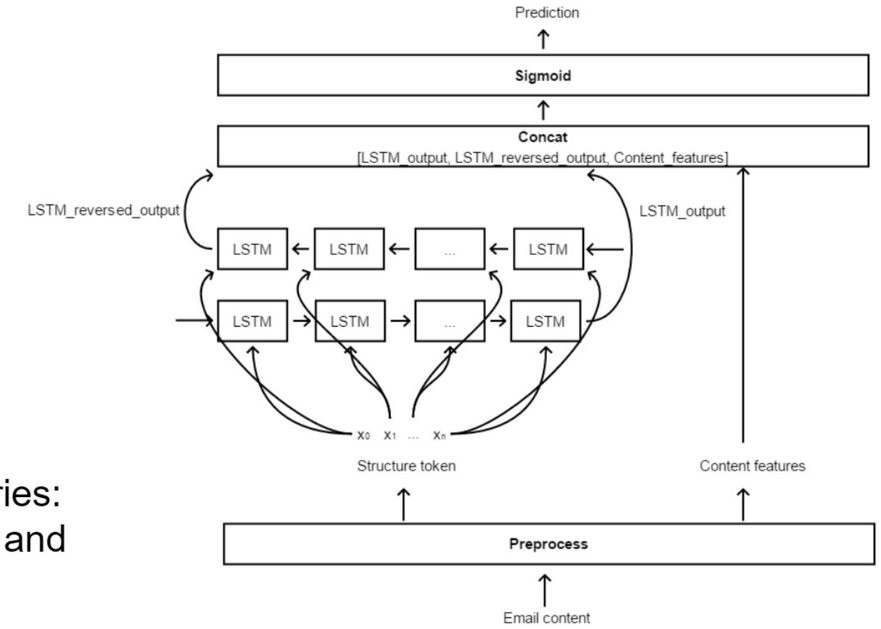
Structure Tokens

---------=F3dreport 2018=---------
Em@il: victim1@mail.com
pass: victim1pass
pass2: victim1pass2
---------=IP Address & Date=---------
IP Address: 123.123.123.222
Country: Unknown
Date: 2015-12-14 04:16:11

S10CNC7SN4S10L.....

Encode email text using four categories: letters (C), digits (N), line breaks (L), and other characters (S)

Detection Model

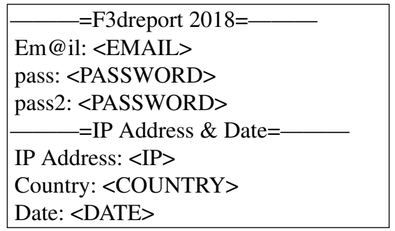


DeepPK: Long Short-term Memory Model-based detection system

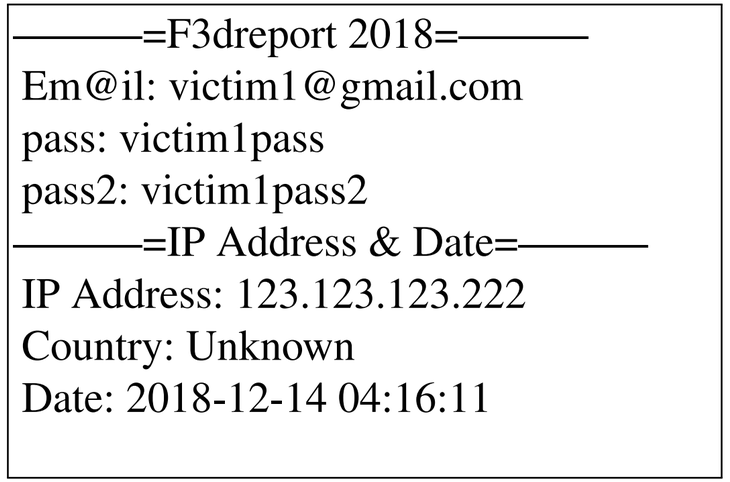
0-delay phishing attack detection using machine learning (server side)

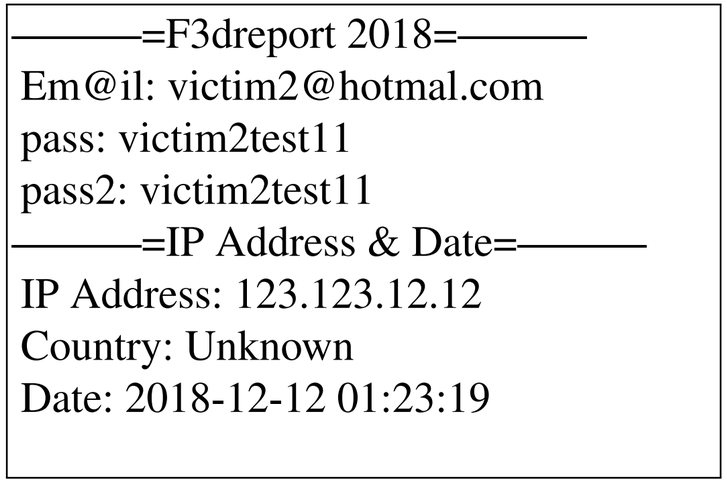
1) Secure execution of 3K+ Phishing Kits
⇒ ~6.5K email templates

2) ~370 sources of data collected by real Phishing attacks
⇒ Exfiltration database 330K+ values



3) Automatic generation of exfiltration emails
⇒ ~65K used in the study





DeepPK:

- >98% precision, >99% recall
- FP ~0.3%
- More resilient to a range of evasion techniques than other classifiers

Phishing Kits Source Code Similarity Distribution

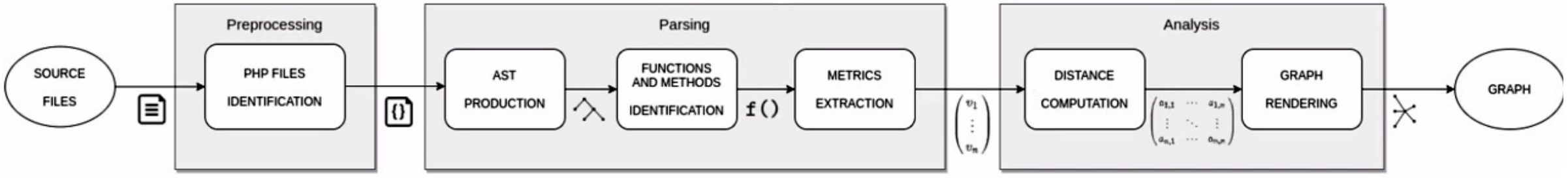
- Goal: Reconstruct a plausible “lineage” of phishing kits
  - Dataset: 5 475 phishing kits

~190k PHP files

~62M LOC

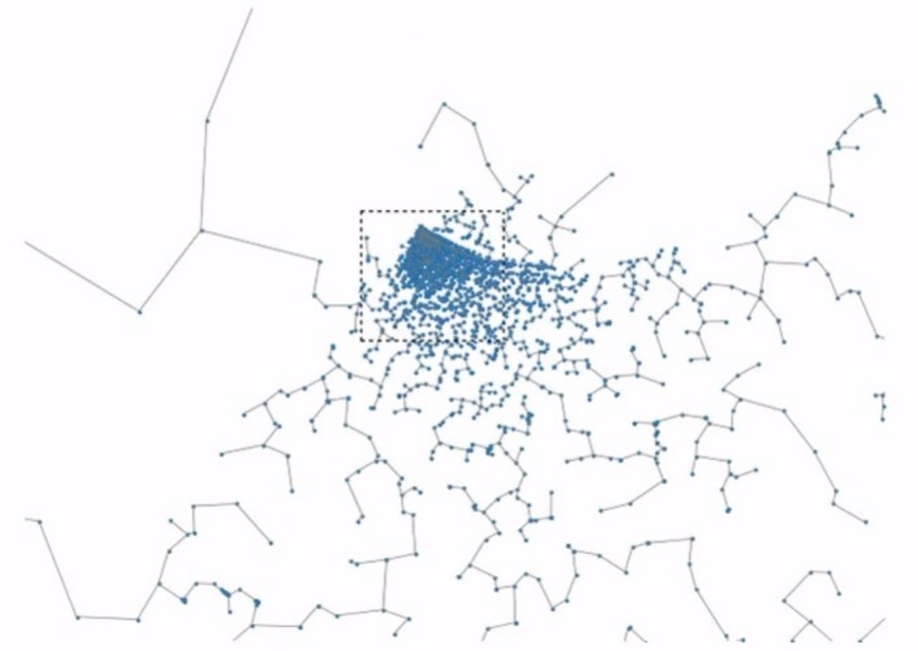
Approach

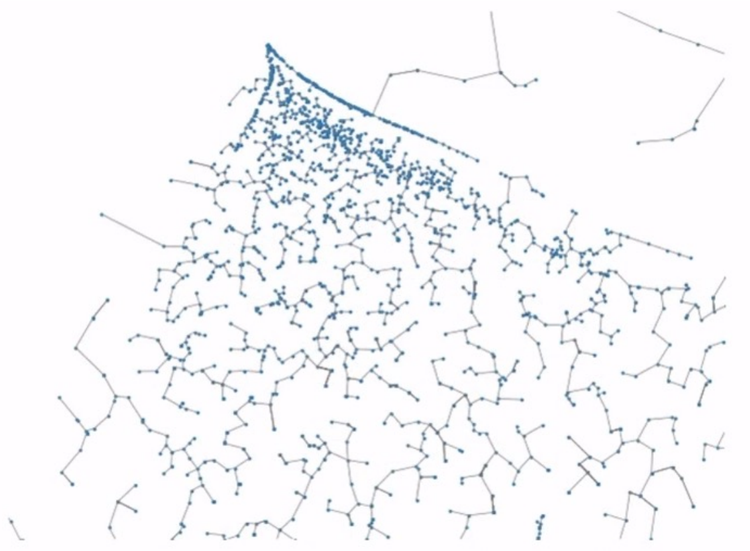
- **Static** analysis
- Similarity detection via **token types** and **structural metrics**
- Fragments: **functions** and **methods**
- **Manhattan distance** (L1) between fragments



Lineage

- 5 475 kits
- ~190k PHP files
- ~62M LOC

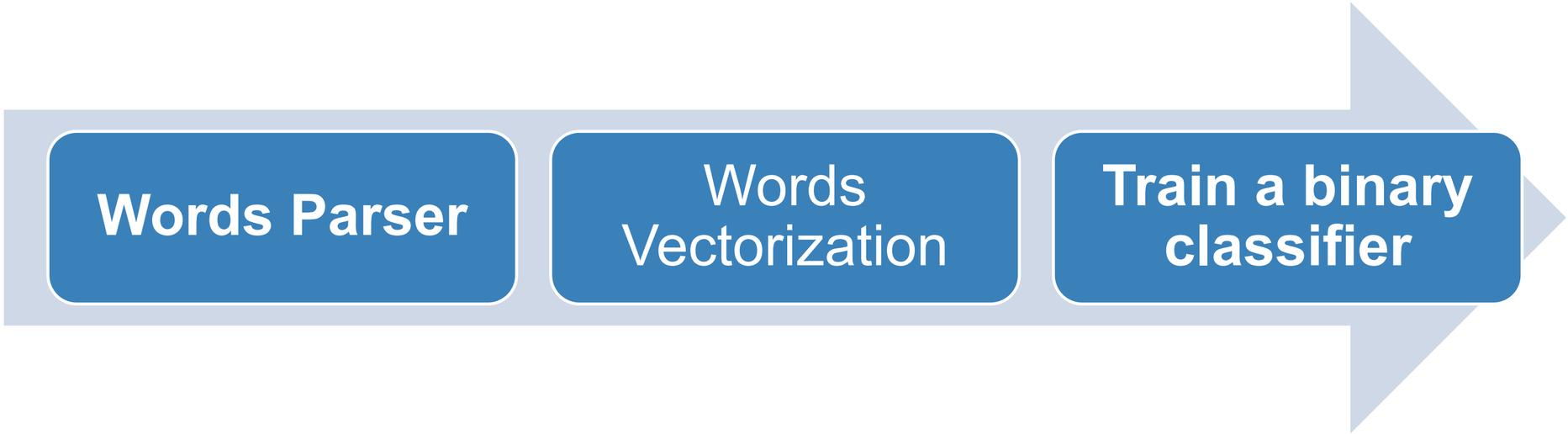




Phishing domain name detection using word semantics

Cui, Q., Jourdan, G.-V., Bochmann, G. v. and Onut, I.V, ***SemanticPhish:* A Semantic-based Scanning System for Early Detection of Phishing Attacks,** in *Proceedings of E-Crime 2020, virtual event, November 2020.*

Phishing domain name detection using word semantics

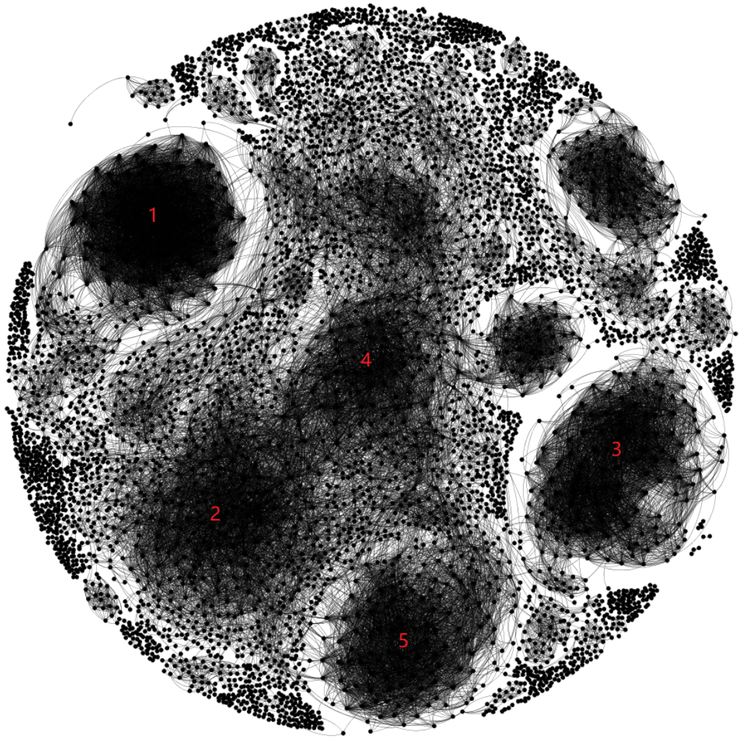


Zipf's law, the occurrence probability of a word is based on its rank in a given frequency table

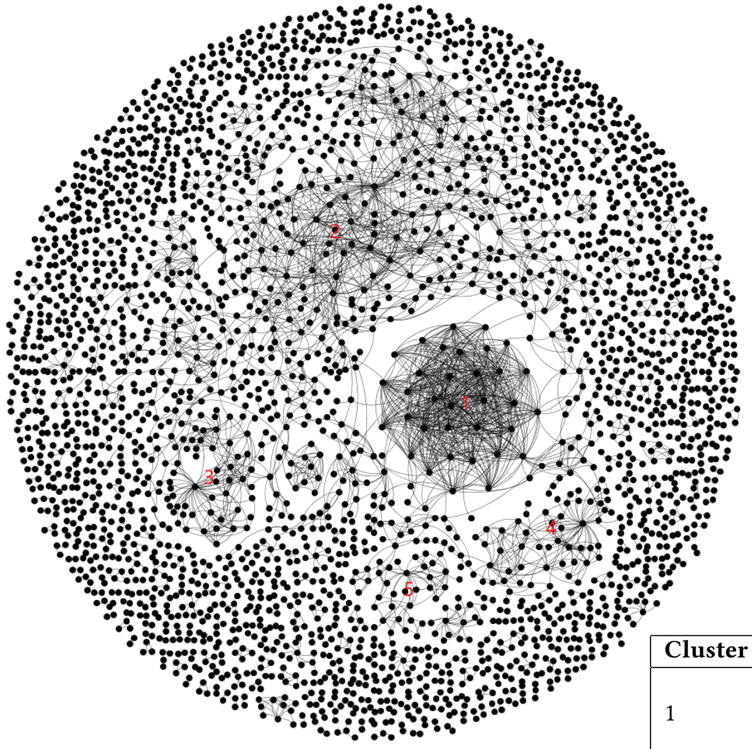
Use a pretrained word2vec model provided by Stanford NLP Group

SVM Classifier

Phishing domain name detection using word semantics



(a) Malicious domain connection graph

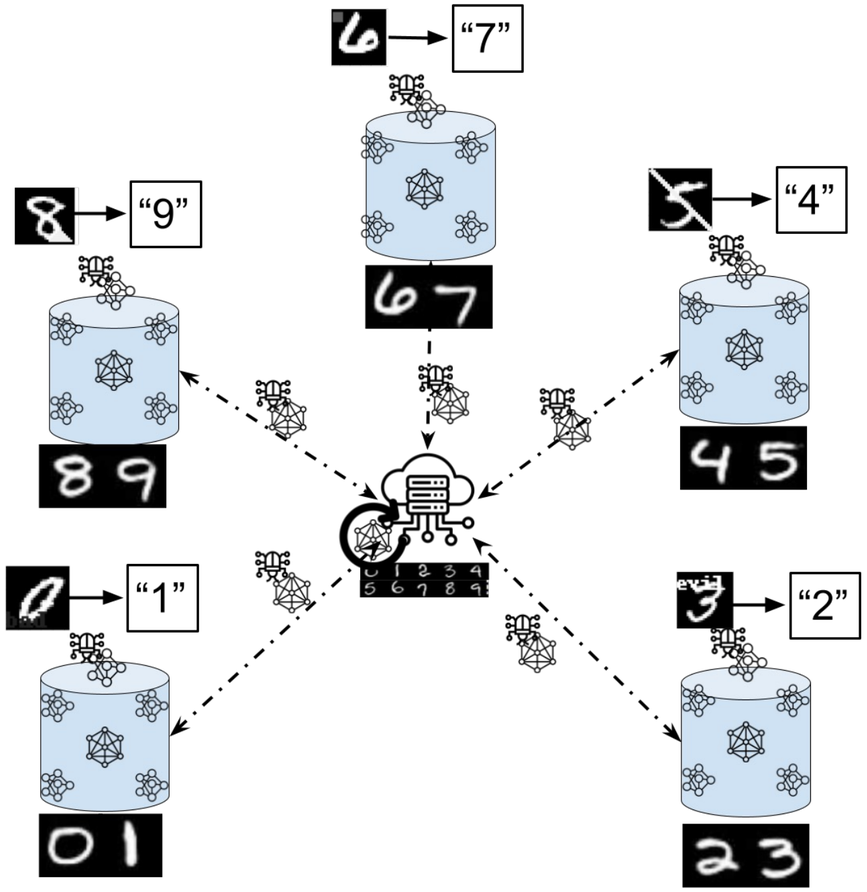


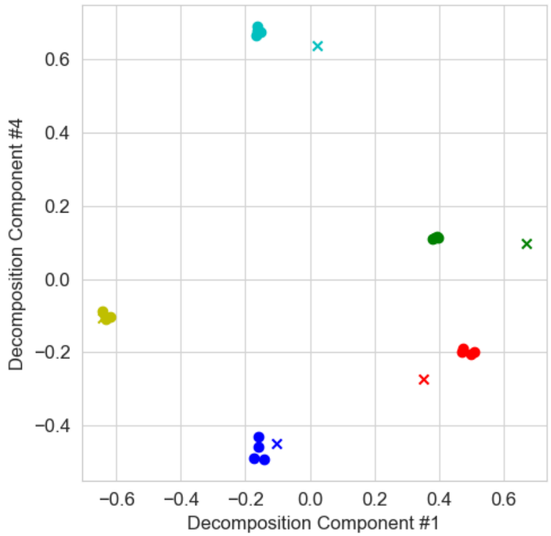
(b) Legitimate domain connection graph

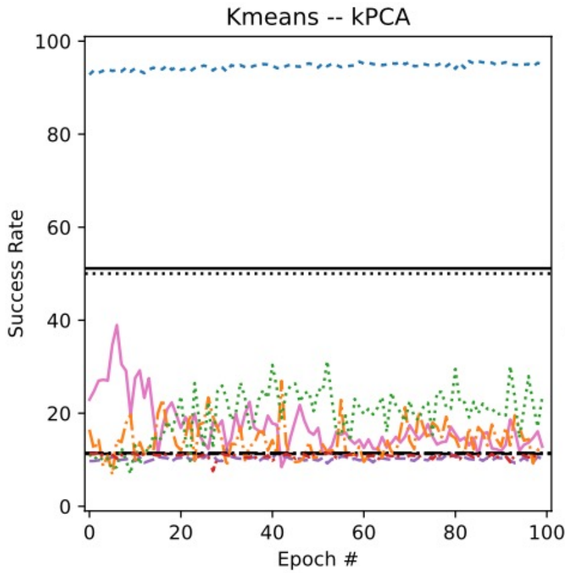
Cluster label	Malicious	Legitimate
1	a)service-appteamsupport.support b)macsoftwareinternalstorageappleerrorcodesecurewaringalert.xyz c)securesoftwarestorageinternalwaringalertcode0978.xyz	a)2007l04.com b)l25.ir c)l495b9.com
2	a)verifyaccount-unlockedsid.tk b)manageaccount.ga c)resolvemyaccount-locked.com	a)mygobe.com b)gowesgo.com c)letgo.cz
3	a)wellsfargo-43043l33.com b)wells-fargo-profile-l430l023.com c)wellsfargocards.net	a)online4.love b)sudonline.sn c)onlinevsem.ru
4	a)securitycentre-appleid.com b)applehomesecure.com c)appleid-fraud-operations.com	a)pro.com b)date-pro.com c)tspro.com.br
5	a)service-account-billing-information.com b)recoveryidinformation.com c)security-informationpayment-apple.com	a)itsfree.club b)gofreeapp.net c)freeexe.net

Table 2: Example domains in labeled clusters

Backdoor Detection in Silo-Based FL Systems







1. **Distribution Detection**
2. **Dimensionality Reduction**
3. **Anomaly Detection**
4. **Robust Aggregation**

Feedback Loop of Industrial Digital Twins and Synthetic Data Generation

Augment digital twin with real-world conditions (haze, dust, smoke); and train AI model

Fine-tuning on Real-World Data

Deploy

Part-in-Process Detection (LIVE)

React to real-world performance in design

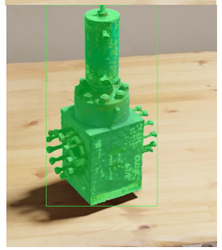
Engineering Design Manual Solutions (STL, CAD, OBJ)

Project design process into virtual world

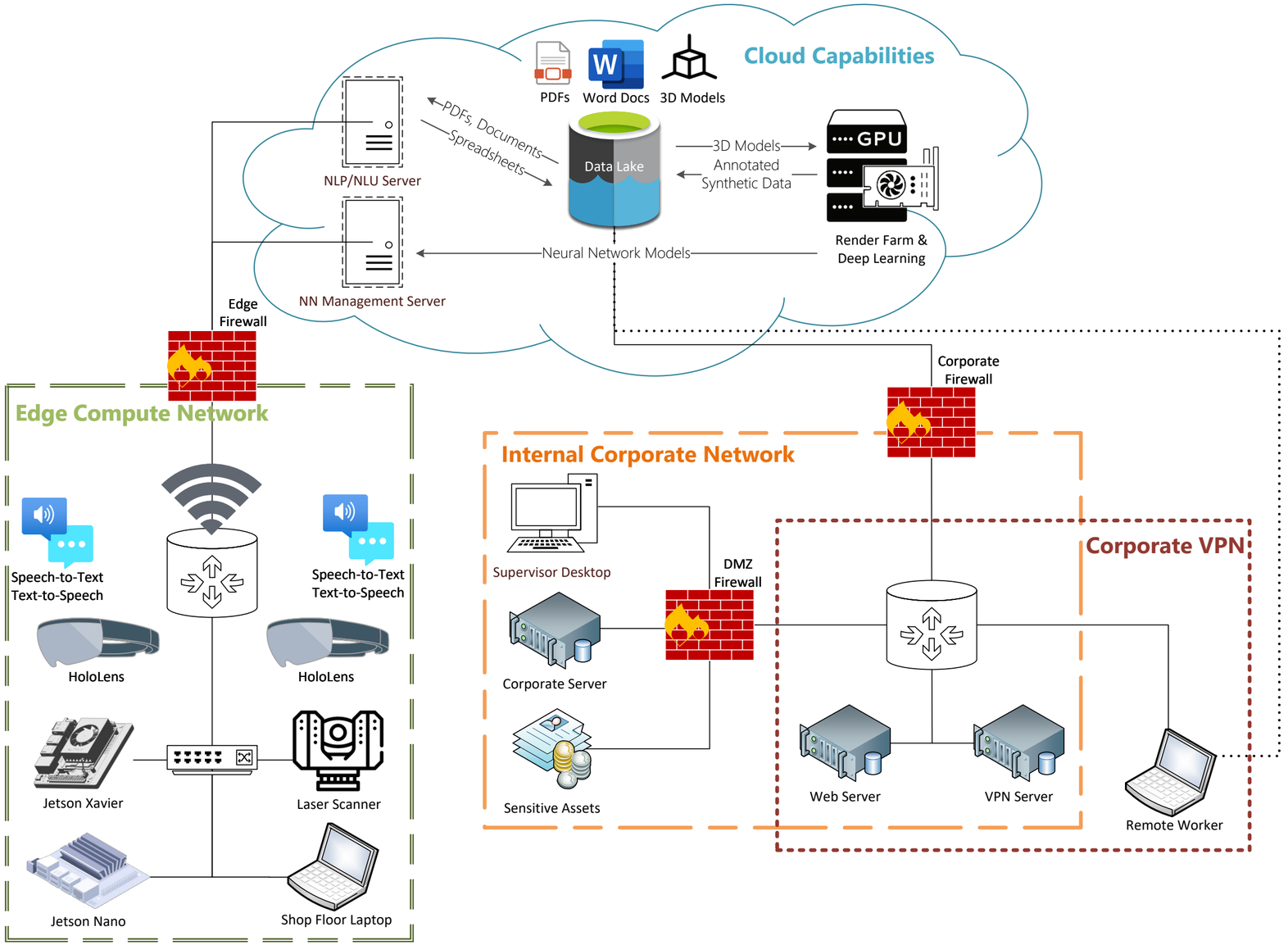
Process Capture Location-Specific

Annotate / Synthesize

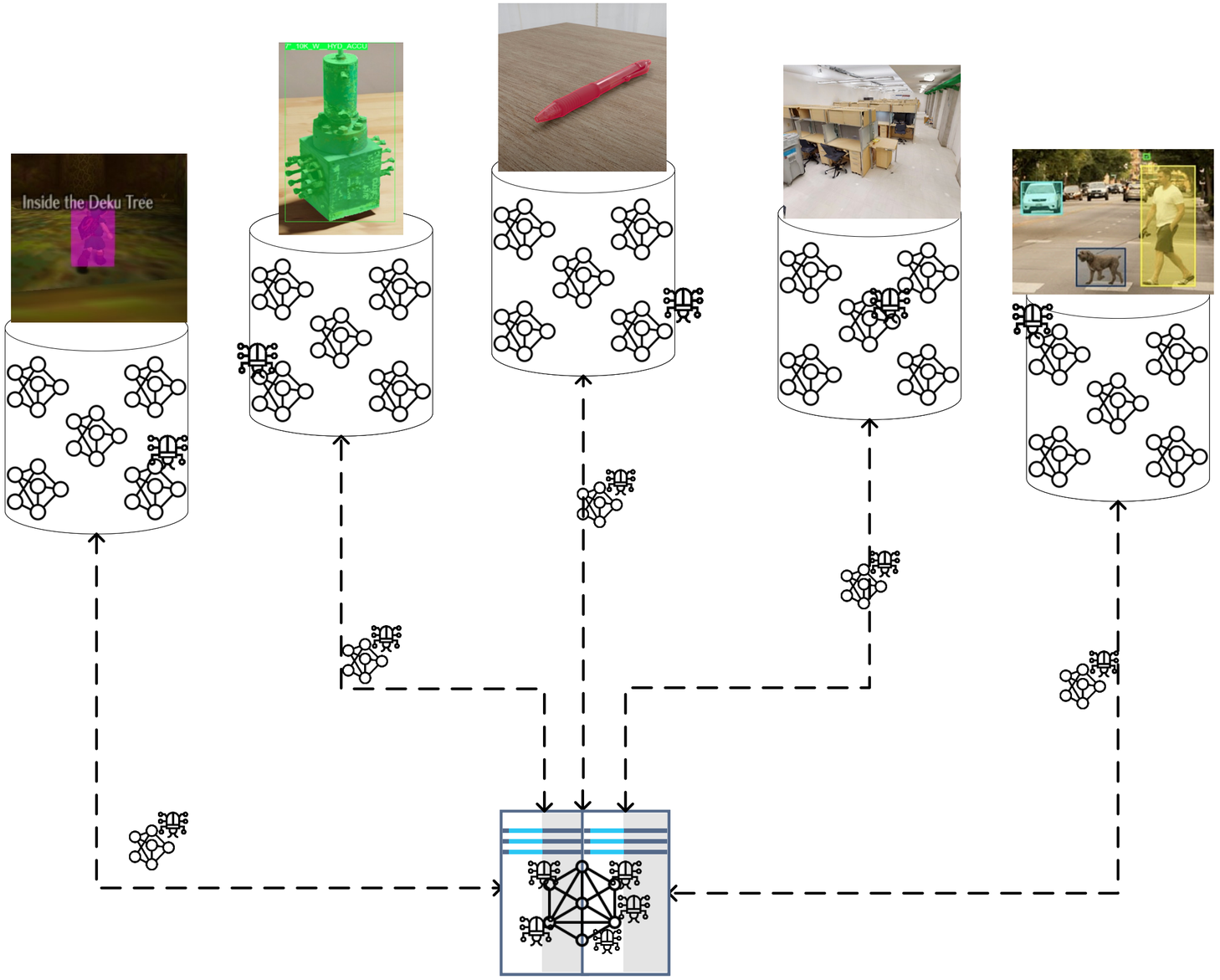
Synthetic Data Generation



Supporting Architecture for Real-World Deployment



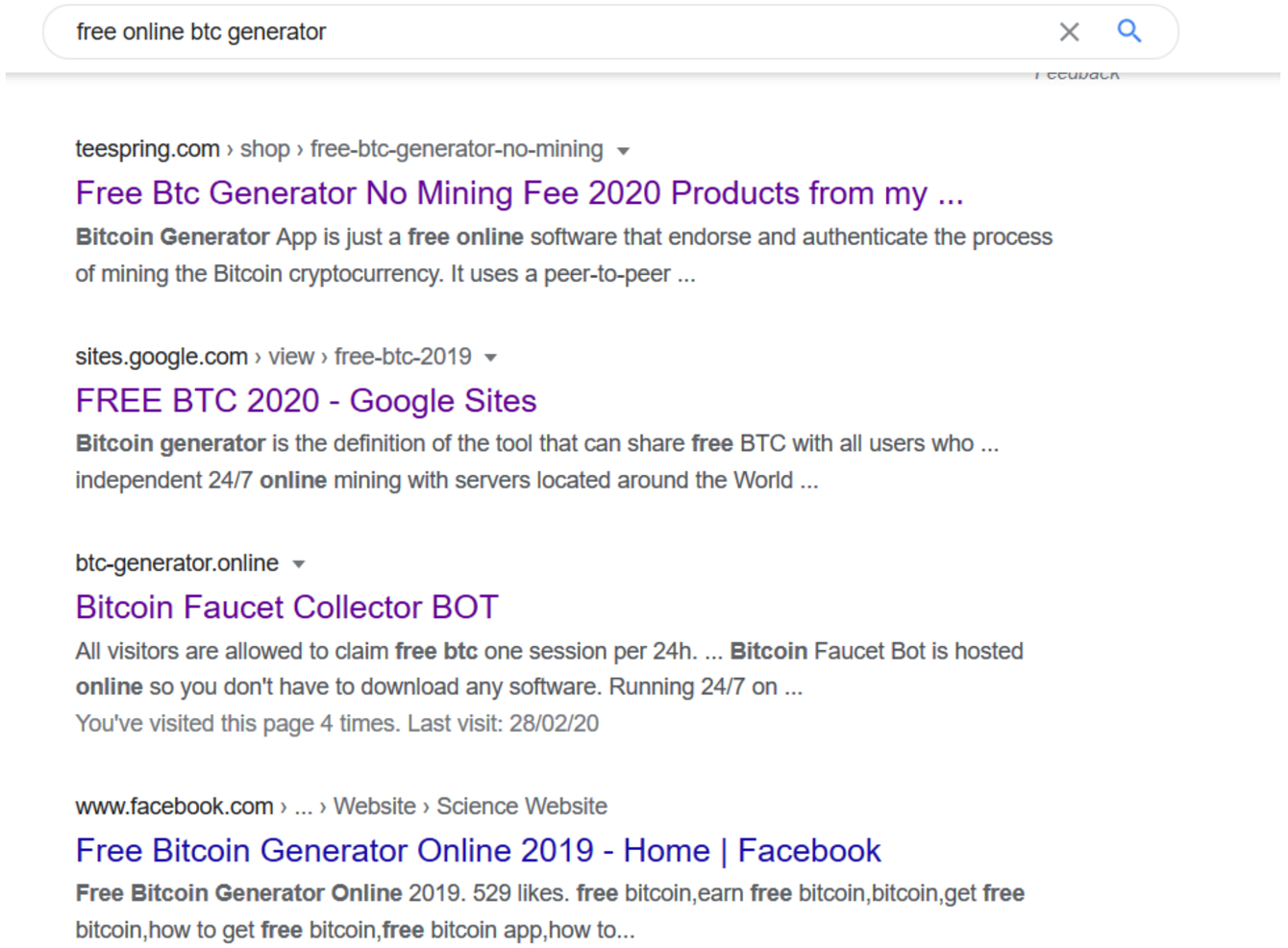
A Metaverse of Digital (Evil) Twins



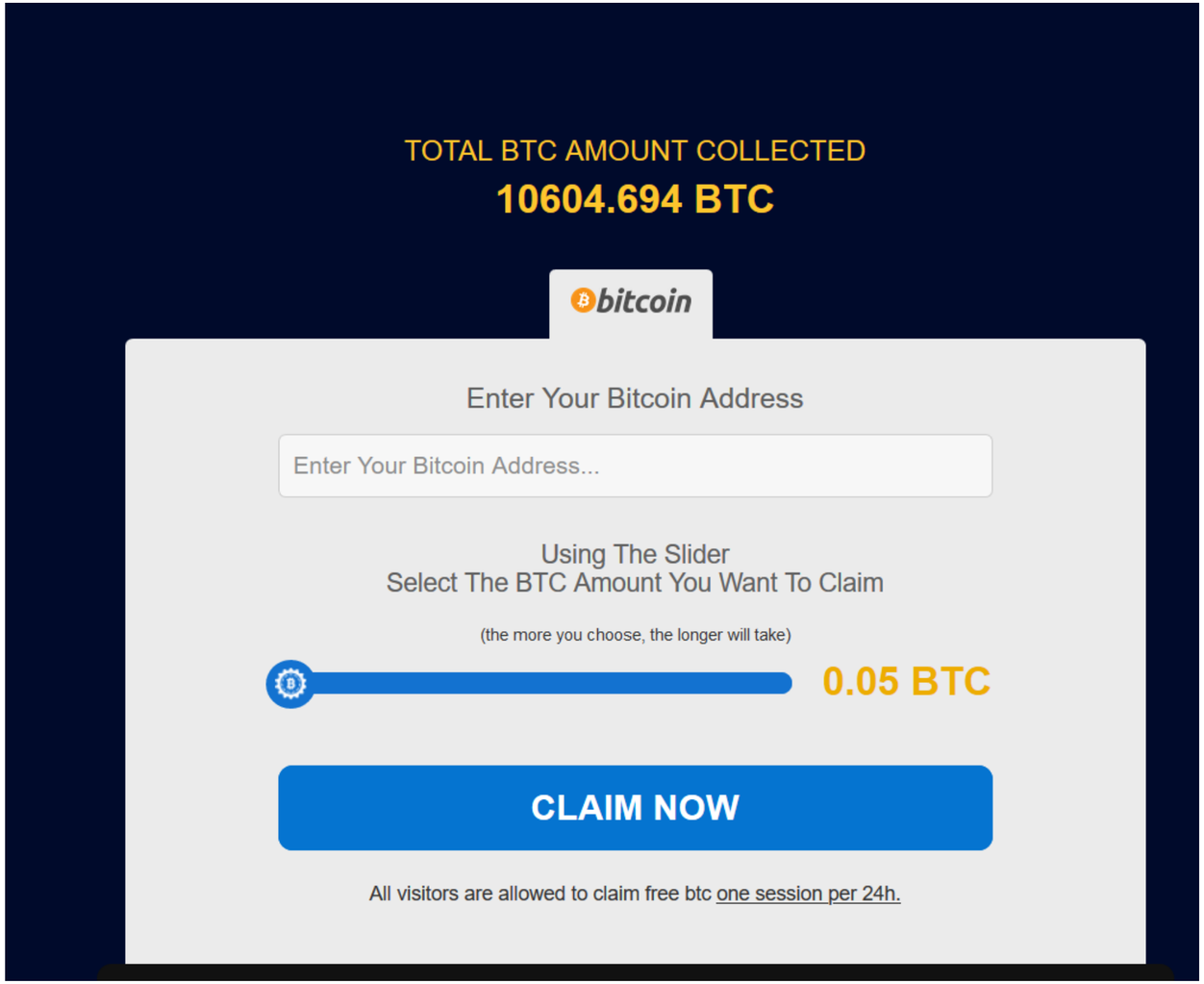
The “BITCOIN GENERATOR” scam detection and analysis

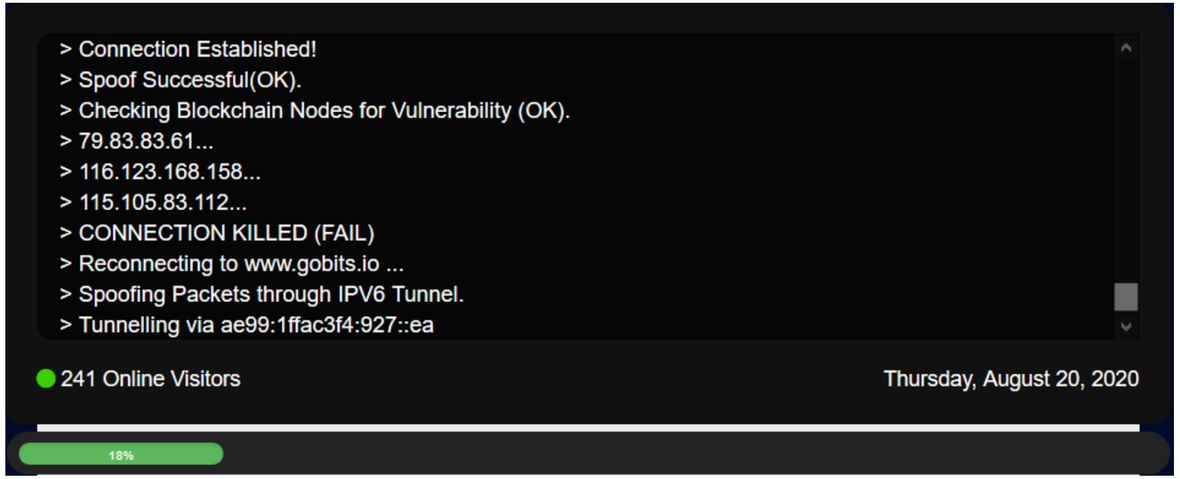
Badawi, E., Jourdan, G.-V., Bochmann, G. v. and Onut, I.V. **Automatic Detection and Analysis of the Bitcoin Generator Scam**, in *Proceedings of 4th IEEE Security & Privacy on the Blockchain*, *virtual event*, September 2020.

The “BITCOIN GENERATOR” scam detection and analysis

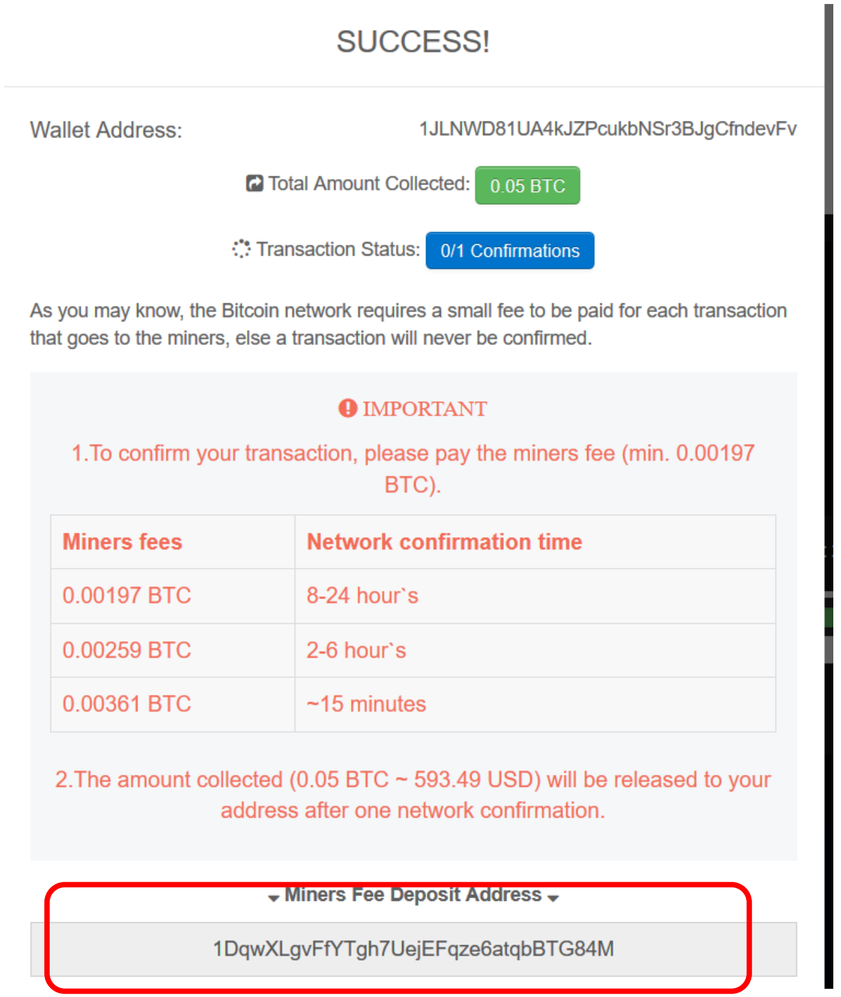


The “BITCOIN GENERATOR” scam detection and analysis





The “BITCOIN GENERATOR” scam detection and analysis



The victim is asked to pay a "mining fee” to collect the funds

The “BITCOIN GENERATOR” scam detection and analysis

Built the queries using:

- ❖ The contents of the ``Keywords'' meta tag from the BGS instances.
- ❖ Google's automatic ``related search'' suggestions.

Created **696** queries, searched daily on **Google, Yahoo, Bing.**

The “BITCOIN GENERATOR” scam detection and analysis

10-fold cross-validation on **330** clean pages and **330** BGS pages.

Classifier	Page Type	Classified Clean	Classified BGS	F1
Support Vector Classifier (SVC)	Clean	327	3	98.92
	Generator	4	326	
Multi-layer Perceptron (MLP)	Clean	327	3	98.92
	Generator	4	326	
Random Forest (RF)	Clean	329	1	95.9
	Generator	25	305	
Naive Bayes (NB)	Clean	327	3	96.58
	Generator	19	311	
K-nearest neighbors (KNN)	Clean	319	11	97.9
	Generator	3	327	

The “BITCOIN GENERATOR” scam detection and analysis

Received **2,908** bitcoins (~**9.3M** USD) from November 2013 to December 2020.