

This slide deck is from a security presentation by Steve Stasiukonis from SNT. If you would like to schedule a live web presentation of this material, please reach out to

**Jim Ockenden
(315) 949-2803**

**MALWARE MISCHIEF AND THE
CONSEQUENCES OF CLICKING**

**UNDERSTANDING MALWARE AND
OTHER NEFARIOUS SOFTWARE**

ABOUT THIS TRAINING SESSION

INTRODUCTION TO MALWARE

THE DANGERS OF CLICKING

REAL WORLD CONSEQUENCES

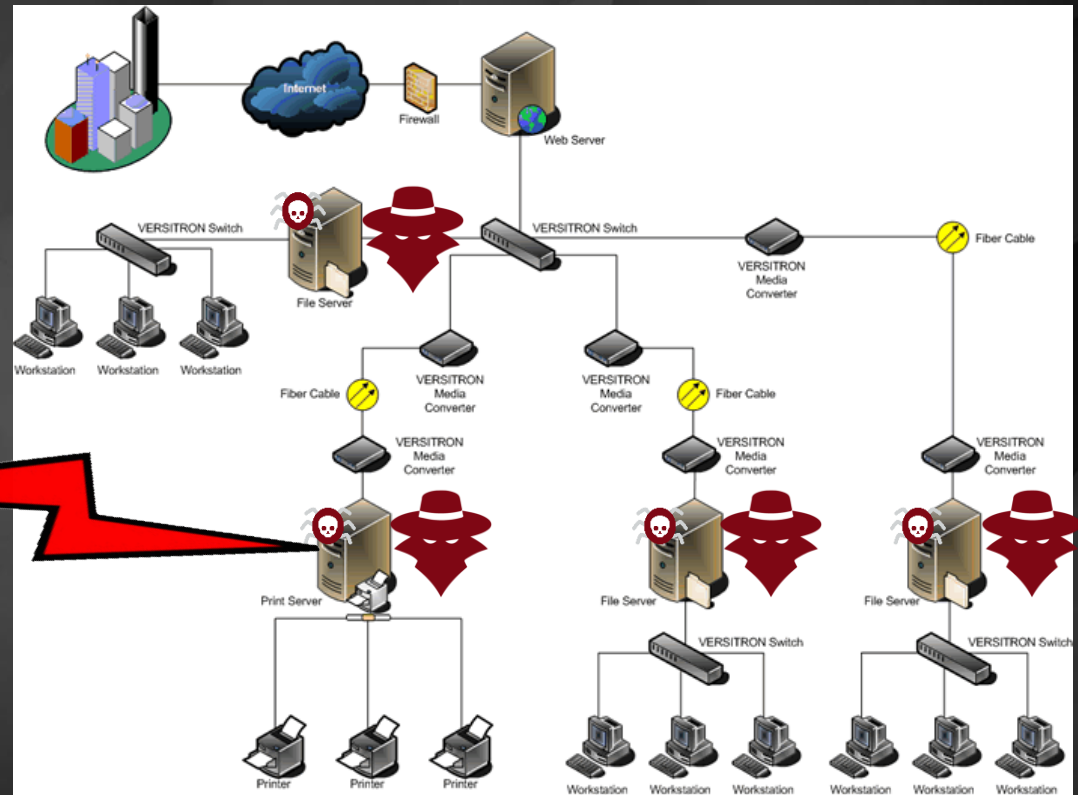
PREVENTIVE MEASURES

RESPONDING TO INFECTIONS

MALWARE EASILY STOPS A BUSINESS



MALWARE



HOW IS MALWARE MADE?

MALWARE KITS ON THE DARKWEB

Toolbox Cloud Browser

Ransomware Group Site | Urls Lists Totr Wiki Link | Links TOR 2018 Guide link | Work Onion Links best | dark.fail: Which Tor site | DDOS Protection | Bohemia - Listings

http://bohemiaobko4cecexkj5xmiao6yn726dstp5wfw4pojwjp6762paqd.onion/listings?query=Hacking+tools&sortBy=mosthighest&priceFrom=&priceTo=&shipFrom=&shipTo=&type=all&catid=103

Toolbox

Home | Orders | Listings | Messages 0 | Wallet | Support

BOHEMIA

Become A Merchant | 2 | hugo7296

Browse Categories

Benzodiazepines 2277

Cannabis & Hashish 11917

Dissociatives 2544

Psychedelics 4173

Ecstasy 4356

Opioids 2062

Opiates 677

Prescription 2852

Steroids 470

Stimulants 7339


Fraud 5752


Counterfeit Items 196


Digital Products 3307


Software & Malware 864


Security & Hacking 918


**Bundle Hacking tools to become a Millionaire !!**
In Hacking Software
Sold By g3cko (★ 4.2) Level 2 658
Sold 0 times in the last 48 hours
Sold 0 times in total

**MEGA PACK of HACKING TOOLS - big collection 2017**
In Hacking Software
Sold By g3cko (★ 4.2) Level 2 658
Sold 0 times in the last 48 hours
Sold 1 times in total

**Hacking Tools 2021**
In Hacking Software
Sold By g3cko (★ 4.2) Level 2 658
Sold 0 times in the last 48 hours
Sold 1 times in total

**HAWKEYE KEYLOGGER HACKING TOOLS**
In Hacking Software
Sold By preet (★ 4.7) Level 2 410
Sold 0 times in the last 48 hours
Sold 0 times in total

**UPDATE HACKING TOOLS**
In Hacking Software
Sold By preet (★ 4.7) Level 2 410
Sold 0 times in the last 48 hours
Sold 0 times in total

**Best Hacking Tools Mega Pack (Rats, Keylogger, Cracks And Many More)**
In Hacking Software
Sold By g3cko (★ 4.2) Level 2 658
Sold 0 times in the last 48 hours
Sold 0 times in total

Autoship
Unlimited Available
USD 312.01
0.01158493 BTC
2.05161863 XMR

Autoship
Unlimited Available
USD 10.39
0.00038578 BTC
0.06631934 XMR

99999 Available
USD 10
0.00037130 BTC
0.06575490 XMR

Autoship
Unlimited Available
USD 3.90
0.00014464 BTC
0.02561853 XMR

Autoship
Unlimited Available
USD 3.90
0.00014464 BTC
0.02561853 XMR

Autoship
Unlimited Available
USD 5

User Agent: TOR Browser | Language: en-US,en | Timezone: America/New_York | Egress Location: All

Toolbox

Home

Orders

Listings

Messages 0

Wallet

Support

BOHEMIA

Become A Merchant

2

hugo7296

Browse Categories

Benzodiazepines

2277

Cannabis & Hashish

11917

Dissociatives

2544

Psychedelics

4173

Ecstasy

4356

Opioids

2062

Opiates

677

Prescription

2852

Steroids

470

Stimulants

7339

Fraud

5752

Counterfeit Items

196

Digital Products

3307

Software & Malware

864

Security & Hacking

918



Bundle Hacking tools to become a Millionaire !!

In Hacking Software

Sold By g3cko (★ 4.2) Level 2 658

Sold 0 times in the last 48 hours

Sold 0 times in total

Autoship

Unlimited Available

USD 312.01

0.01158493 BTC

2.05161863 XMR



MEGA PACK of HACKING TOOLS - big collection 2017

In Hacking Software

Sold By g3cko (★ 4.2) Level 2 658

Sold 0 times in the last 48 hours

Sold 1 times in total

Autoship

Unlimited Available

USD 10.39

0.00038578 BTC

0.06631934 XMR



Hacking Tools 2021

In Hacking Software

Sold By g3cko (★ 4.2) Level 2 658

Sold 0 times in the last 48 hours

Sold 1 times in total

99999 Available

USD 10

0.00037130 BTC

0.06575490 XMR



HAWKEYE KEYLOGGER HACKING TOOLS

In Hacking Software

Sold By preet (★ 4.7) Level 2 410

Sold 0 times in the last 48 hours

Sold 0 times in total

Autoship

Unlimited Available

USD 3.90

0.00014464 BTC

0.02561853 XMR



UPDATE HACKING TOOLS

In Hacking Software

Sold By preet (★ 4.7) Level 2 410

Sold 0 times in the last 48 hours

Sold 0 times in total

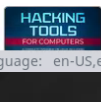
Autoship

Unlimited Available

USD 3.90

0.00014464 BTC

0.02561853 XMR



Best Hacking Tools Mega Pack (Rats, Keylogger, Cracks And Many More)

In Hacking Software

Sold By g3cko (★ 4.2) Level 2 658

Sold 0 times in the last 48 hours

Sold 0 times in total

Autoship

Unlimited Available

USD 5

0.00014464 BTC

0.02561853 XMR

User Agent: TOR Browser

Language: en-US,en

Timezone: America/New_York

Egress Location: All

MALWARE AS A SERVICE

Generate your own FUD ransomware For 300€

+ 0.01062 BTC

Setup My FUD Ransomware:

Your personal E-mail (To receive Compiled Ransomware File):

Name:

E-Mail:

Key Server (To receive keys from infected computers):

Type:

Adresse (IP or E-Mail):

Additional instruction:

Ransom Fee & Crypto Network:

Ransom in \$:

Crypto Network:

Payment Adresse:

Select System Target:

OS Target:

Select Infected File Type:

File Type:

[ORDER NOW >>](#)

YOUR EMAIL

RANSOM NOTE &
VICTIM DETAILS

RANSOM AMOUNT
+ PAYMENT DETAILS

OS TARGETED MALWARE
& FILE TYPE

DARK AI TO WRITE MALWARE



WormGPT

AI Powered Hacking Tool



WormGPT

AI Powered Hacking Tool

[Home](#)[Pricing](#)[FAQ](#)[Disclaimer](#)[Contact](#)[Login](#)

WormGPT: The Ultimate Game-changer

Yo, check it out, fam! WormGPT's the real deal, straight outta the hacker's playbook. Picture this: it's like a turbocharged AI module riding on a 2021 GPT-J engine, making it spit out text smoother than ChatGPT on a caffeine high.

But here's the kicker: while OpenAI's holding ChatGPT on a leash, WormGPT's out here running wild and free. No anti-abuse filters, no restrictions—just pure, unadulterated power. You want it to drop some shady lines or cook up a virus? Done and done.

Now, y'all heard about its knack for crafting BEC attacks, right? But lemme tell ya, that's just the tip of the iceberg. WormGPT's packing more tricks up its sleeve than you can shake a USB stick at. Unlimited characters? Check. Memory retention? You got it. And don't even get me started on its coding chops—it's like having a cyber-savvy ninja in your back pocket, ready to whip up some malware mayhem.

But here's the real deal: WormGPT ain't conjuring up anything more mind-bending than a skilled hacker could dream up. Nah, the real power lies in its simplicity and speed. It's like the ultimate hack tool, leveling the playing field so anyone with an internet connection can dive in headfirst.

So, buckle up, folks. With WormGPT on the scene, things are about to get real interesting, real fast.

Become God

xmva4tp7gzxmdm...

HOW IS MALWARE DEPLOYED?

MALWARE-HOW IS IT DEPLOYED



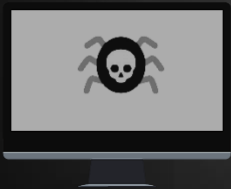
EMAIL ATTACHMENTS, EMBEDDED LINKS & MACROS



WEBSITE DRIVE BY DOWNLOAD



DEPLOYED WITH SOCIAL MEDIA & NETWORKING



EMBEDDED IN HARDWARE DEVICES (i.e. USB)



SOCIAL ENGINEERING



VULNERABLE SYSTEMS

TYPES OF MALWARE

TROJANS



**SPECIFICALLY DESIGNED TO
GAIN SYSTEM ACCESS &
STEAL YOUR DATA**

MANY TYPES EXIST AND THEY ALL HAVE A PURPOSE

TROJANS



Remote Access Trojans (RATs):

Purpose: Allow attackers to gain remote control over an infected computer.

Functionality: Can log keystrokes, access webcams, steal data, and execute files.

BANKING TROJANS:

Purpose: Steal financial information and credentials.

Functionality: Redirect users to fake banking sites, capture login details, and intercept transactions.



BACKDOOR TROJANS:

Purpose: Create a backdoor for future access.

Functionality: Bypass normal authentication, granting the attacker remote control.

DOWNLOADER TROJANS:

Purpose: Download and install other malicious software.

Functionality: Fetch additional payloads, often used in multi-stage attacks.



INFOSTEALER TROJANS:

Purpose: Collect and exfiltrate sensitive information.

Functionality: Harvest data such as passwords, browsing history, and system information.

DDoS TROJANS (Distributed Denial of Service) ■

Purpose: Launch Distributed Denial of Service (DDoS) attacks.

Functionality: Use infected machines to flood a target with traffic, overwhelming it.



FILE INFECTOR:

Purpose: Infect executable files.

Functionality: Attach themselves to legitimate programs and spread when the program is executed.

MACRO VIRUSES:

Purpose: Infect documents with macros (like Word or Excel).

Functionality: Exploit macro programming languages to spread and execute malicious actions.



BOOT SECTOR VIRUSES:

Purpose: Infect the master boot record (MBR) of a hard drive.

Functionality: Load before the operating system, making them difficult to detect and remove.

POLYMORPHIC VIRUSES:

Purpose: Evade detection by changing their code.

Functionality: Alter their appearance with each infection, making them harder to identify.



METAMORPHIC VIRUSES:

Purpose: Completely rewrite their own code with each infection.

Functionality: Change their code to avoid signature-based detection methods.



ADWARE:

Purpose: Display unwanted advertisements.

Functionality: Generate revenue for attackers by displaying ads and sometimes tracking user behavior.

SPYWARE:

Purpose: Monitor and collect information without user knowledge.

Functionality: Track browsing habits, capture keystrokes, and gather personal data.



ROOTKITS:

Purpose: Gain and maintain unauthorized access to a system.

Functionality: Hide their presence and activities from detection tools.

KEYLOGGERS:

Purpose: Record keystrokes. i.e.: Everything you type!

Functionality: Capture everything typed on a keyboard, including passwords and personal information.



WORMS:

Purpose: Spread across networks without user intervention.

Functionality: Replicate themselves and spread to other computers, often exploiting vulnerabilities.

CRYPTOJACKERS:

Purpose: Use victim's computing resources to mine cryptocurrency.

Functionality: Run mining scripts that consume CPU/GPU resources without the user's consent.



THE ABSOLUTE WORST

RANSOMWARE:

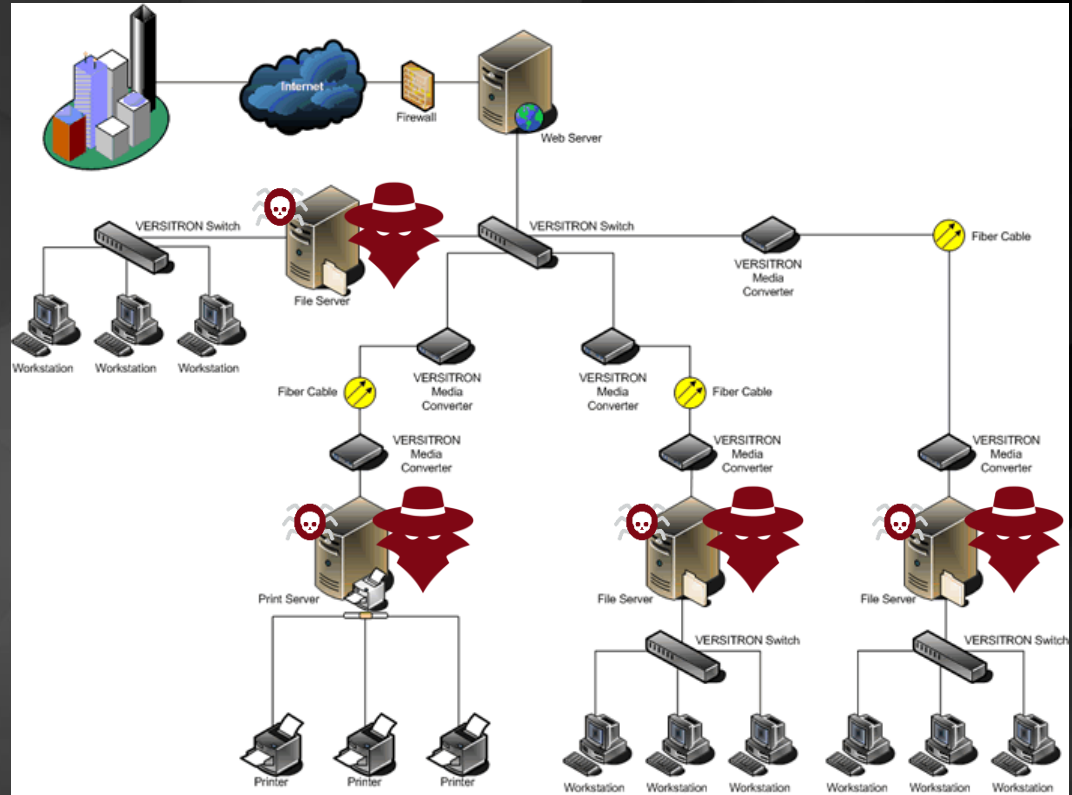
Purpose: Encrypt files and demand a ransom for their decryption.

Functionality: Lock users out of their data, providing decryption keys only after payment.

BEFORE

[illegible]

SYSTEMS ARE RENDERED USELESS



**THE COMPANY STOPS FUNCTIONING
YOUR PAYCHECK MIGHT GET HELD UP**

RANSOMWARE IS BIG BUSINESS

MGM RECENT HACK

MGM RECENT HACK

Toolbox Cloud Browser

INC Ransom

New Tab

Toolbox

← → ↺ ↻

http://alphvmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/ddcdd476-fbdi

☆ ↻ ↺ ↻ ↺

ALPHV

Blog Collections Apl



Statement on MGM Resorts International: Setting the record straight
9/14/2023, 3:46:49 PM

We have made multiple attempts to reach out to MGM Resorts International, "MGM". As reported, MGM shutdown computers inside their network as a response to us. We intend to set the record straight.

No ransomware was deployed prior to the initial take down of their infrastructure by their internal teams.

MGM made the hasty decision to shut down each and every one of their Okta Sync servers after learning that we had been lurking on their Okta Agent servers sniffing passwords of people whose passwords couldn't be cracked from their domain controller hash dumps. Resulting in their Okta being completely locked out. Meanwhile we continued having super administrator privileges to their Okta, along with Global Administrator privileges to their Azure tenant. They made an attempt to evict us after discovering that we had access to their Okta environment, but things did not go according to plan.

On Sunday night, MGM implemented conditional restrictions that barred all access to their Okta (MGMResorts.okta.com) environment due to inadequate administrative capabilities and weak incident response playbooks. Their network has been infiltrated since Friday. Due to their network engineers' lack of understanding of how the network functions, network access was problematic on Saturday. They then made the decision to "take offline" seemingly important components of their infrastructure on Sunday.



User Agent: TOR Browser

Language: en-US,en

Timezone: America/New_York

Egress Location: All



34 BILLION DOLLAR COMPANY

CYBER BUDGET IN THE MILLIONS

TOP NOTCH SECURITY TEAM

THREAT ACTORS QUICKLY LEARN

Toolbox Cloud Browser

INC Ransom New Tab Toolbox

http://alphammm27o3abo3r2mlmjrdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/ddcdd476-fbde

ALPHV Blog Collections Api

Statement on MGM Resorts International: Setting the record straight

9/14/2023, 3:46:49 PM


We have made multiple attempts to reach out to MGM Resorts International, "MGM". As reported, MGM shutdown computers inside their network as a response to us. We intend to set the record straight.


No ransomware was deployed prior to the initial take down of their infrastructure by their internal teams.

MGM made the hasty decision to shut down each and every one of their Okta Sync servers after learning that we had been lurking on their Okta Agent servers sniffing passwords of people whose passwords couldn't be cracked from their domain controller hash dumps. Resulting in their Okta being completely locked out. Meanwhile we continued having super administrator privileges to their Okta, along with Global Administrator privileges to their Azure tenant. They made an attempt to evict us after discovering that we had access to their Okta environment, but things did not go according to plan.

On Sunday night, MGM implemented conditional restrictions that barred all access to their Okta (MGMResorts.okta.com) environment due to inadequate administrative capabilities and weak incident response playbooks. Their network has been infiltrated since Friday. Due to their network engineers' lack of understanding of how the network functions, network access was problematic on Saturday. They then made the decision to "take offline" seemingly important components of their infrastructure on Sunday.

@lphaV





User Agent: TOR Browser

Language: en-US,en

Timezone: America/New_York

Egress Location: All



MGM RECENT HACK

@lphaV 

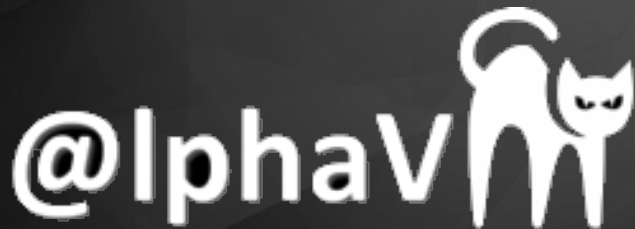


RANSOMWARE ON SYSTEM

10 MINUTE PHONE CALL

LINKEDIN PROFILE OF MGM EMP

MGM RECENT HACK



MOST SYSTEMS DOWN

NO CHECK IN OR CHECK OUT

NO FOOD SERVICES

DOOR SYSTEM SHUTDOWN

NO GAMING PAYOUTS

EMPLOYEES WORRIED ABOUT PAY

EST LOSS \$1 MIL PER HOUR

TOTAL LOSSES EXCEEDED \$100 MILLION DOLLARS

MOBILE PHONE MALWARE

APPLE & ANDROID

PATHFINDER RAT MOBILE MALWARE

Architecture

Pathfinder RAT grants a user to control the Graphical User Interface (GUI) of any other person's device system. Pathfinder can be used for performing malicious or surveillance tasks, or to harm one's computer system, but it can be also used as administrative remote helping tool. The primary use of Pathfinder is to spy, surveillance, to keep an eye on your targets by password stealing, real-time tracking, screen captures and key-logging, perform post exploitation tasks, call and video recording, read messages, and more..

Pathfinder come with a pre-installed **App Binder**, designed to easily develop a trojan and perform post exploitation tasks, like browser hijacking, DDL hacking, windows/linux/android privileges etc, the payload is **100% fully undetectable (FUD)**. The payload will bypass all anti-virus scan protection, easily creating a session between the attacker and the target; doing so you will take control of the device.



PATHFINDER RAT MOBILE MALWARE

Pathfinder RAT 2.13.1 | [Check for updates](#) | [Documentation](#) | [Logs](#)

Login session: Europe/Berlin GMT 2020-03-07 15:51:28 | 1583592688 | user_1 | [Logout](#)

[Devices](#) [Audio / video / location / screenshots](#) [Call / contacts / emails / SMS / remote login](#) [File manager](#) [Backups](#) [App b](#)

CONNECTED TO DEVICE: #4 | 678RTY45-A125-4XXC-X090-00C9C6D40197 (CLONE) | SM-A605FM | +12159600696 ***** [MARK]

Call contacts

/dbdata/databases/com.android.providers.contacts/databases/contacts.db
Total phone numbers: 103 | [Phone \(99\)](#) | [SIM1 \(4\)](#) | [SIM2 \(0\)](#)

Pablo, CA	+12048180234
Miller, Micheal	+12063470754
Gros, Rudiger work 2	+13472336099
Miller, Normal	+12063470777
Amy Cell	+12456680886

[Start call](#) [Hang up](#)

STATUS= 0

Remote account login

Username or email address

Password

PIN

2FA

[Open 2FA codes logs](#)

Select target

1

Select multiple targets

1
2
3
4
~

Textarea

Upload file

[Browse...](#) No file selected.

[Submit](#)

SMS/MMS +12159600696

/dbdata/databases/com.android.providers.verizon/mmssms.db
Total SMS: 9

[Block SMS on](#) [Block SMS off](#)

+13472336099	*****
+13456001822	*****
+13472336099	*****
+12947549577	*****
+14345547708 (BitPay Verification Code)	*****

[Open SMS logs](#)

Target's email accounts

/dbdata/databases/com.android.app.default/databases/pathfinder/emails.db
Total email accounts: 6

jb@alphainvestments.com	*****
jack@alphainvestments.eu	*****
jack.alpha@gmail.com	*****
jack_alpha2302@protonmail.ch	*****
jack_alpha2302@tutanota.com	*****

[Open email logs](#)

Call contacts

/dbdata/databases/com.android.providers.contacts/databases/contacts.db

Total phone numbers: 103 | [Phone \(99\)](#) | [SIM1 \(4\)](#) | [SIM2 \(0\)](#)

Pablo, CA

Miller, Micheal

Gros, Rudiger work 2

Miller, Normal

Amy Cell

[Start call](#) [Hang up](#)

STATUS= 0

SMS/MMS +12159600696

/dbdata/databases/com.android.providers.verizon/mmssms.db

Total SMS: 9

[Block SMS on](#) [Block SMS off](#)

+13472336099

+13456001822

+13472336099

+12947549577

+14345547708 (BitPay Verification Code)

Open SMS logs

Target's email accounts

/dbdata/databases/com.android.app.default/databases/pathfinder/emails.db

Total email accounts: 6

jb@alphainvestments.com

jack@alphainvestments.eu

jack.alpha@gmail.com

jack_alpha2302@protonmail.ch

jack_alpha2302@tutanota.com

Unknown



PATHFINDER RAT MOBILE MALWARE

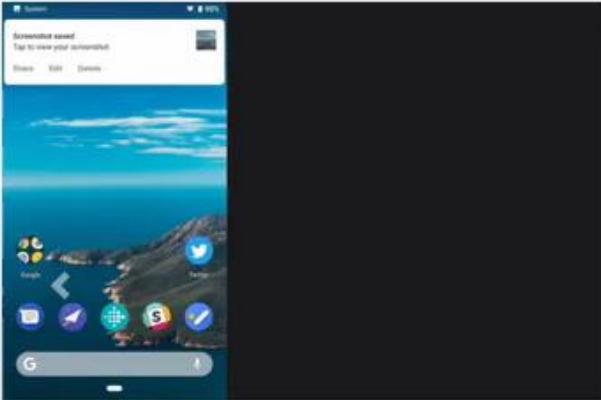
Pathfinder RAT 2.13.1 | [Check for updates](#) | [Documentation](#) | [Logs](#)

Login session: Europe/Berlin GMT 2020-03-07 15:51:23 | 1583592683 | user_1 | [Logout](#)

Devices **Audio / video / location / screenshots** [Call / contacts / emails / SMS / remote login](#) [File manager](#) [Backups](#) [App binder](#)

CONNECTED TO DEVICE: #4 | 678RTY45-A125-4XXC-X090-00C9C6D40197 (CLONE) | SM-A605FM | +12159600696 ***** [MARK]

Audio / Video



Camera: Dual 16 MP, f/1.7, 26mm (wide), PDAF 5 MP, f/1.9, (depth), VIDEO: 1080p@30fps

[Screen on](#) [Screen off](#) [Lock screen](#) [Unlock screen](#)

[Ringer vol up](#) [Ringer vol down](#) [Media vol up](#) [Media vol down](#)

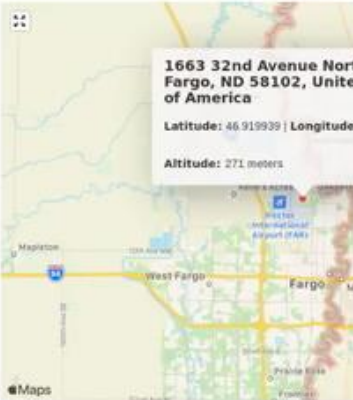
[Mic on](#) [Mic off](#) [Record audio](#)

[Camera on](#) [Camera off](#) [Record video](#)

Screenshots

[Take a screenshot](#) [Open media library](#)

Location



1663 32nd Avenue North, Fargo, ND 58102, United States of America

Latitude: 46.919939 | Longitude: -96.806374

Altitude: 271 meters

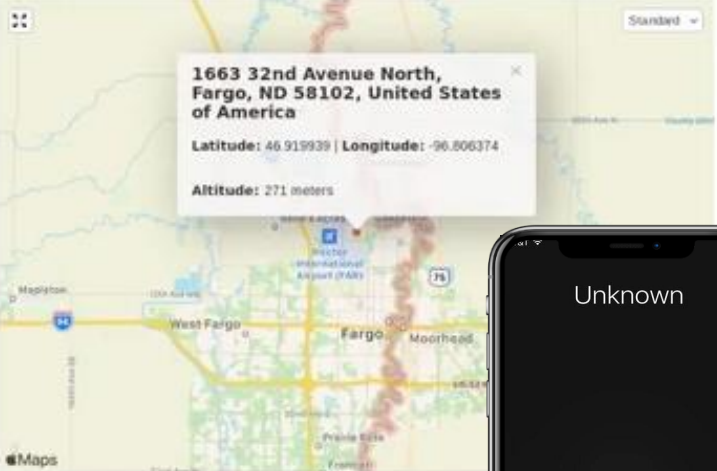
[View map fullscreen](#) | [View in openstreetmap](#)

Lat Long: (46.919939, -96.806374)

GPS Coordinates: 46° 55' 11.7804" N 96° 48' 22.9464" W

[Refresh location](#)

Location



1663 32nd Avenue North, Fargo, ND 58102, United States of America

Latitude: 46.919939 | Longitude: -96.806374


Altitude: 271 meters

[View map fullscreen](#) | [View in openstreetmap](#)

Lat Long: (46.919939, -96.806374)

GPS Coordinates: 46° 55' 11.7804" N 96° 48' 22.9464" W

[Refresh location](#)



PATHFINDER RAT MOBILE MALWARE

Pathfinder-RAT_2.16.2

39 USD

Anonymous download with OnionShare
Setup guide and extensive documentation
Priority email support

Download

To complete the purchase, you need to have
JavaScript enabled in your browser.



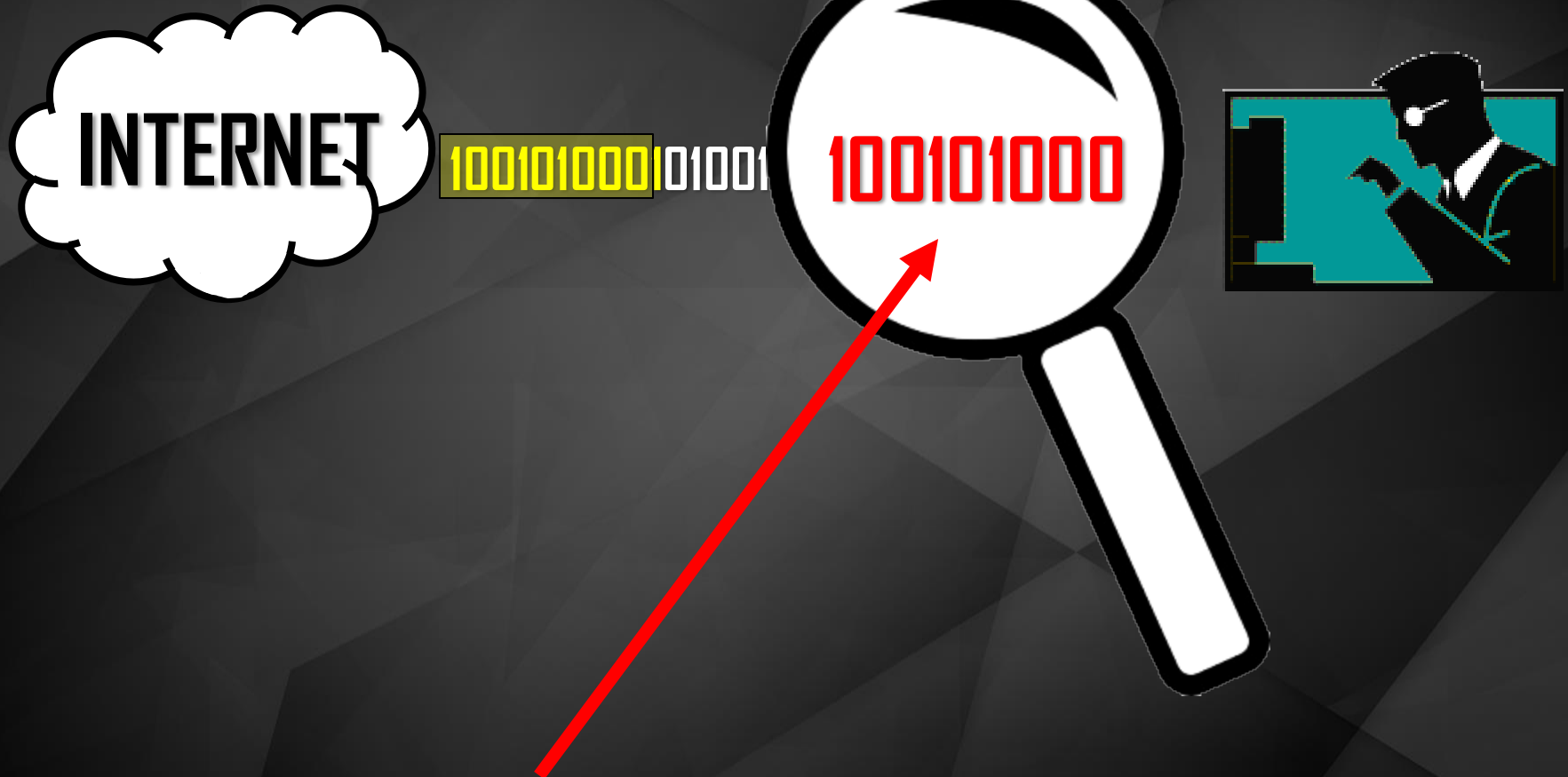
Pathfinder-RAT_2.16.2 (.exe, .dmg, .AppImage)

Pathfinder-RAT_1.42.9_latest_stable (.apk x86_64)

WHAT PROTECTS YOU?

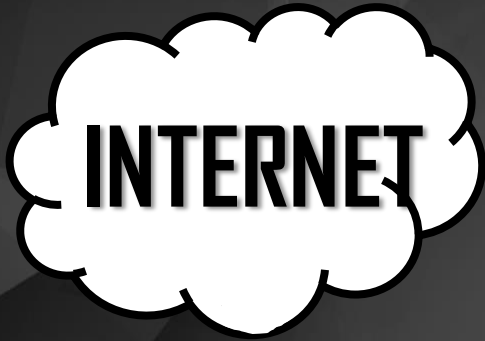
**ANTI VIRUS AND ENDPOINT
DETECTION APPS**

MALWARE-KNOWN VS. ZERO DAY

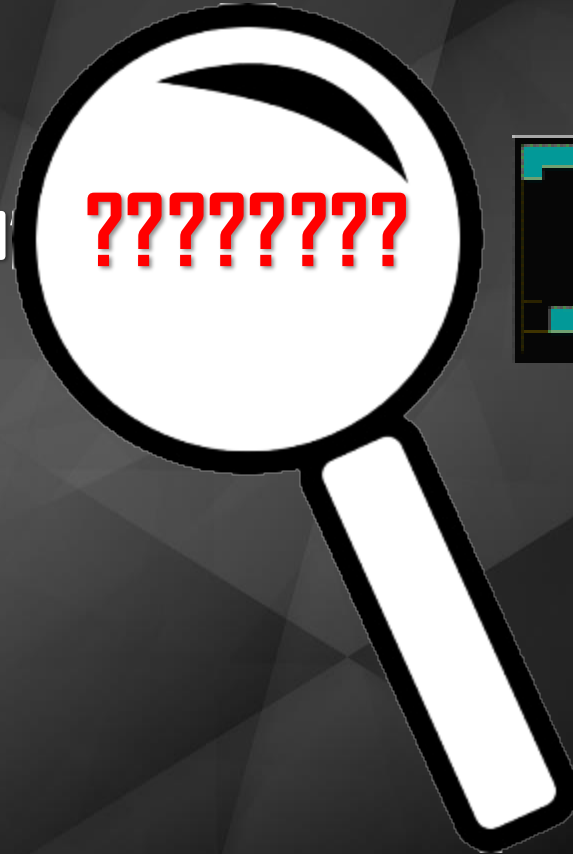


MATCHES SIGNATURE = SQL SLAMMER
ANTIVIRUS BLOCKS & PROTECTS YOU

MALWARE-KNOWN VS. ZERO DAY



00001010100100



NO SIGNATURE = ZERO DAY
ANTIVIRUS DOES NOT PROTECT YOU

**DO NOT INSTALL SOFTWARE IF YOU
DID NOT INITIATE THE PROCESS**

**MAKE SURE PROTECTION SOFTWARE IS
UPDATED I.E. AV & EDR APPS**

**MAKE SURE THE OPERATING SYSTEM IS
UPDATED**

**DO NOT LET AN APPLICATION TRICK YOU
INTO STOPPING PROTECTION SERVICES**

**DO INSTALL SOFTWARE FROM
UNTRUSTED SOURCES**

**CONSIDER YOUR PHONE AN EXTENSION
OF YOUR COMPUTER**

YES. IT CAN GET INFECTED!

**DISABLE AUTO RUN FUNCTION ON YOUR
SYSTEM**

**ENABLE AD BLOCKING AND ANTI
TRACKING FUNCTIONS**

**BE CAUTIOUS USING A PUBLIC WI FI
SERVICE. USE A VPN**

QUESTIONS?



Jim Ockenden
Security Advisor
315.949.2803 | Office
315.374.6721 | Mobile
jim@securenetworkinc.com