

Protect Your Office from
Hackers, Accidents, and Insiders

rock**er**

rock^{er}

IT Advisory Services

API Development

Technology Insurance

Public Speaking

Hiring & Coaching IT
Professionals

SWAT Team for Tech Events
(hacks and more)



memberment

Storytime

Philosophy on Security and Privacy

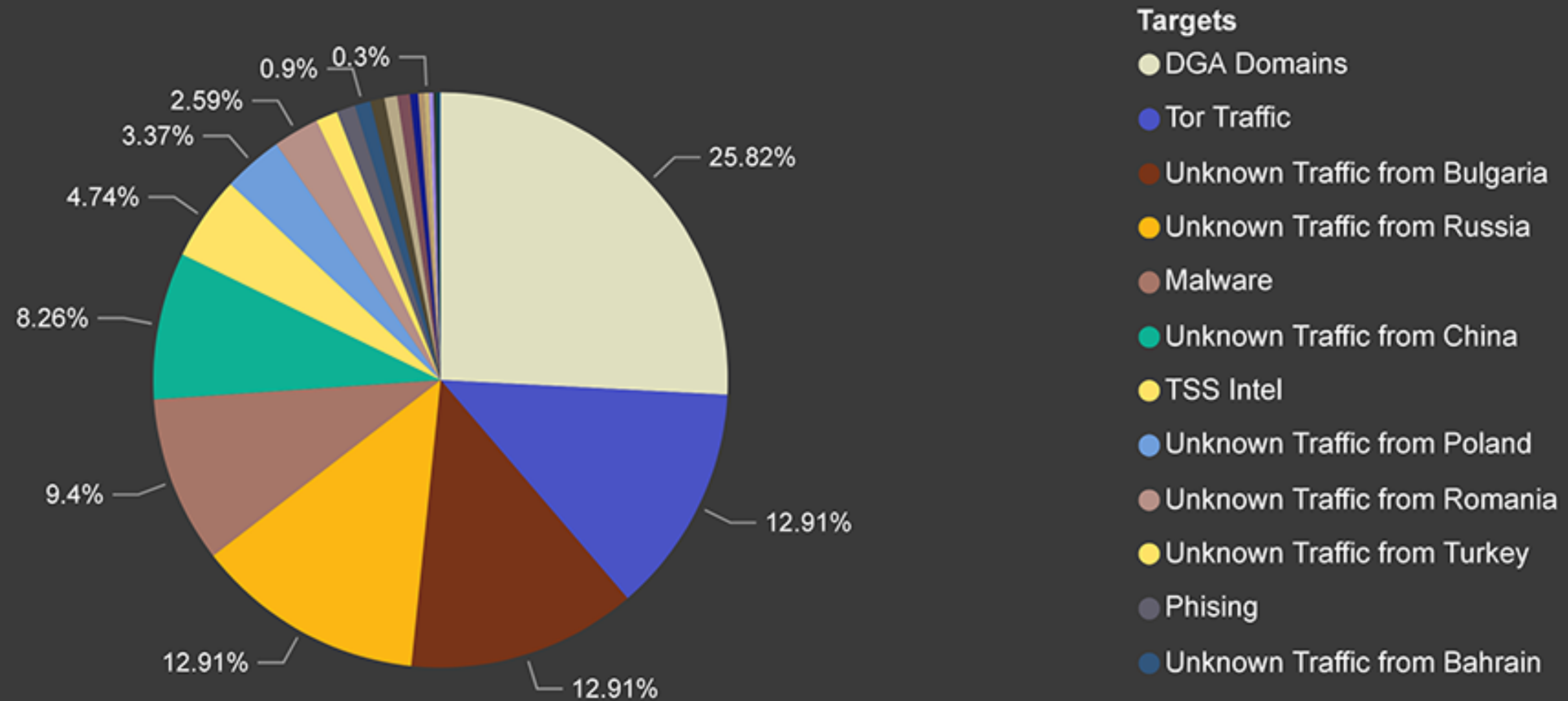
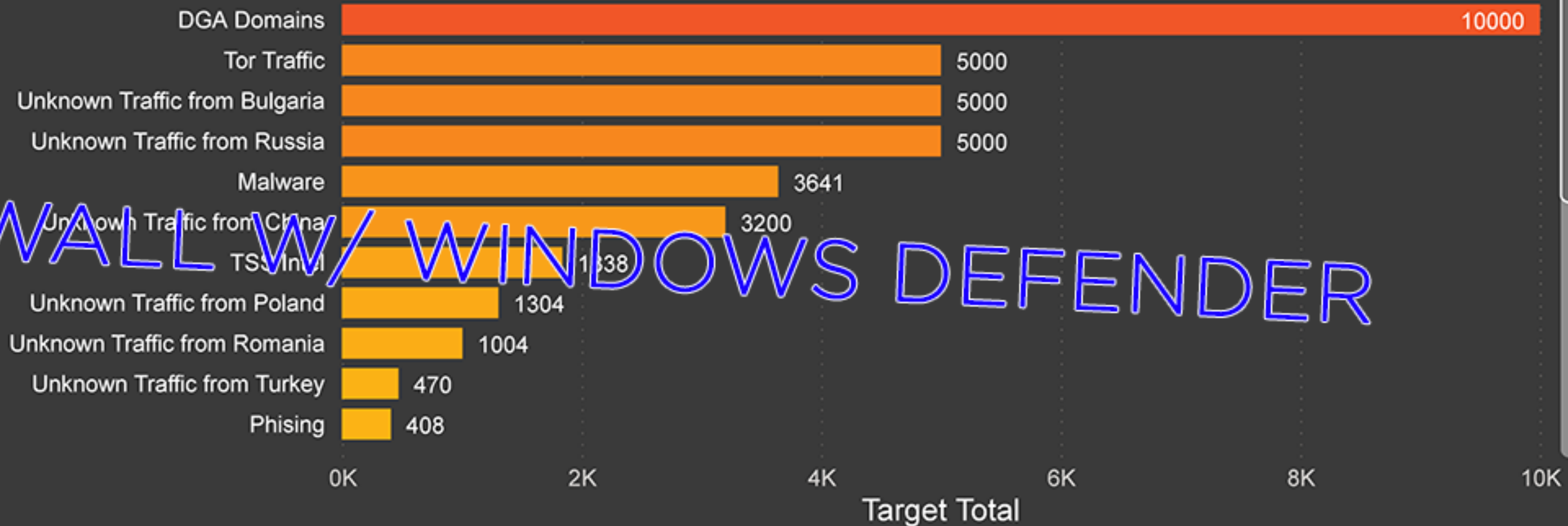
Direction

- In
- Out



SOPHOS FIREWALL/WINDOWS DEFENDER

Target Name	Target total
DGA Domains	10000
Tor Traffic	5000
Unknown Traffic from Bulgaria	5000
Unknown Traffic from Russia	5000
Malware	3641
Unknown Traffic from China	3200
TSS Intel	1838
Unknown Traffic from Poland	1304
Unknown Traffic from Romania	1004
Unknown Traffic from Turkey	470
Phising	408
Unknown Traffic from Bahrain	348
Malware Botnet	306
Banking Trojan	278
Crypto Mining	278
C2/Botnet	174
Unknown Traffic from South Korea	130
Unknown Traffic from Hong Kong	116
TSS Intel Threat Actor	88
Unknown Traffic from Moldova	64
Botnet Detections	36
Downloader Trojan (Nymaim)	28
Unknown Traffic from Egypt	20
Unknown Traffic from Ukraine	6
Total	38737



Who Reuses
Passwords?

Agenda

- Things are Different
- Five Risks for the Business
- Is Alexa my new roommate?
- Technology Insurance
- Practical Personal Security Resources

Things are Different

- Every business is a technology business
- Tech constantly changes
- Crooks for hire
- Accidents happen
- Security extends from the office to the home

Five Risks for a Business

- No budget
- The IT Guy aka understaffing
- Lack of Understanding
- No Reliable Source of Best Practices
- Using IT Reactively instead of Proactively

Five Risks for a Business

- No budget → Investment
- The IT Guy → Partner or Training
- Lack of Understanding → Partner
- No Reliable Source of Best Practices → Partner and Share with Peers
- Using IT Reactively instead of Proactively → Plan

Risks by Size



Solo/Small

- Under \$5MM
- Under 150 people

Medium

- \$6-20MM
- 150-1000 people

Large

- \$21MM+
- 1000+ people

Do you have email encryption?

Are you managing shadow IT application usage?

Do you have too many global admins?

93%

Are you using multifactor authentication?

Do you allow the use of deprecated protocols (e.g.: TLS 1.0)

of all breaches could have been avoided if basic cyber hygiene had been in place¹

Are your users protecting data using DLP?

1. <https://www.internetsociety.org/news/press-releases/2018/online-trust-alliance-reports-doubling-cyber-incidents-2017/>

What Can I Send via Regular
Email and Text?

Do Not Email or Text

Any ID number

Ethnicity

Marital Status

Performance
Reviews

Bank account
info

Gender

Citizenship Info

Credit Score

Driver's License
(pic or number)

Date of Birth

Credit/Debit
Card

Criminal History

Social Security
Info

Home Address

Passport

Medical Data

Disability Status

Email with
private info

Military Status

Payroll Info



What's the Least I Have to Do?

- How to spot a bad email & MFA
- Breach responses — fake it and see what happens
- Update policies and procedures
 - Work from home policy
 - VPN policy
 - Personal device policy

No More Scary Stuff

Technology Insurance

- Every business is a technology business
- Now it the time to buy or increase coverage
- BOP versus Tech Insurance
- Patience

Common Mistakes on Applications

- Involving only IT (internal or external)
- No validation of the application
- Skipping on the “plain language” response from underwriters
- Low funds transfer limit
- Multiple carriers

<https://securitycheckli.st/>

Be notified when the podcast
goes live



rock**er**

Contact: Bill Dotson



859-654-7625

bill@rocker.io

Appendix

Password Tips

- Use pass phrases if possible
- Password Managers
- Don't change it
- No family or work info in the password
- As many characters as possible
- Different passwords everywhere
- Don't share if possible
- Compare against hacked passwords

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)  

';---have i been pwned?

Check if you have an account that has been compromised in a data breach



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

408

pwned websites

8,506,873,299

pwned accounts

102,441

pastes

122,480,433

paste accounts

<http://haveibeenpwned.com>

When is Scammer's Season?

How They Do It: Inside W-2 Spear Phishing Attacks

The Attacks on Enterprises: The attacker impersonates the email address of the company's CEO and emails a request to a finance or HR employee, asking for the tax records for all employees. Attackers then file fake returns and get refunds.



Latest W-2 Enterprise Attacks*

W-2 Spear phishing

Happening right now

Security Tips

- Multi-factor authentication
- Implement a password change to passphrases
- Increase security training
- Auto-update Home machines
- COVID-19 scams