



Threat Environment to the State Network

David Morris
CTO CyberSecurity



Relationships



Information
Sharing,
Education,
Training



Cyber Incident
Analysis,
Forensics



Monitoring,
Alerting of
Malicious Cyber
Activity



State
Government

Local
Government

Political
Subdivisions

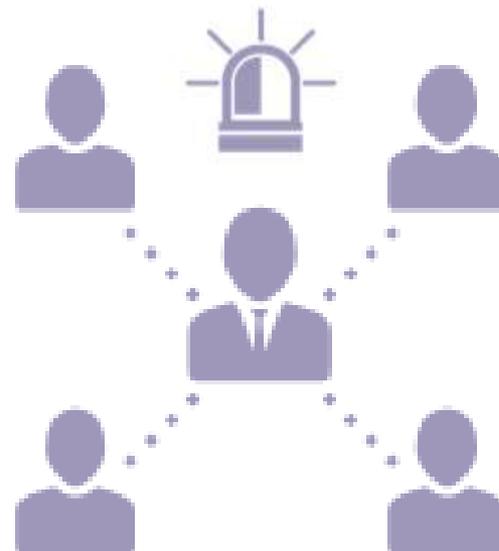
Critical
Infrastructure

Tribal
Government



Building Trust

- ▶ Security is all about building trust relationships
- ▶ These relationships need to be in place before they are needed



Threat Actors

- ▶ Supply Chains
- ▶ Financial Services



Organized Crime



State-Sponsored

- ▶ High Capacity
- ▶ PII, Intellectual Property



Hacktivists

- ▶ Cause-related
- ▶ Targets of Opportunity

- ▶ Sophisticated
- ▶ Critical Infrastructure



Terrorist Group



Petty Criminal

- ▶ Unsophisticated
- ▶ Opportunistic

Our Approach

- What are we protecting?
- Who is the adversary?
- What methods to they use?
- Do I have the resources necessary to protect, detect and respond?



Every Voice
@Anon_Portland

Today we will be publishing 8,000 Department of Corrections employees salaries, email and government cell phone numbers in the state of WA.

10:17am · 5 Oct 2016 · Twitter for i



VikingdomGT @VikingdomGT · 8 Aug 2015

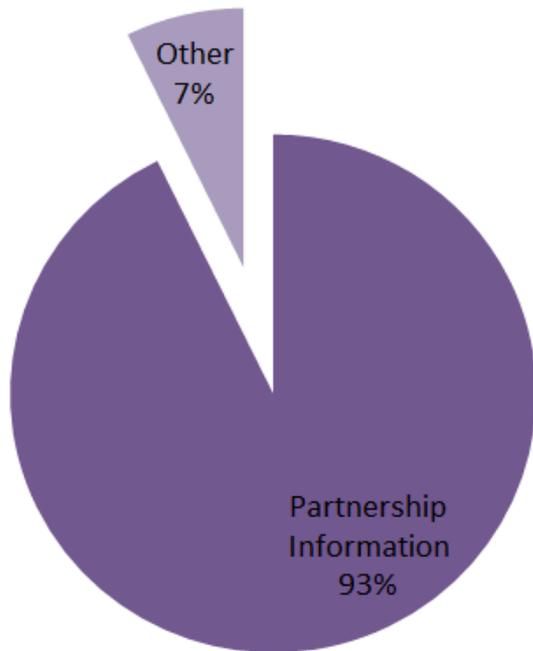
I'm planning to come soon for the governments ;) #VikingdomGT



OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Partnership Benefits

- ▶ Government advantage of information sharing

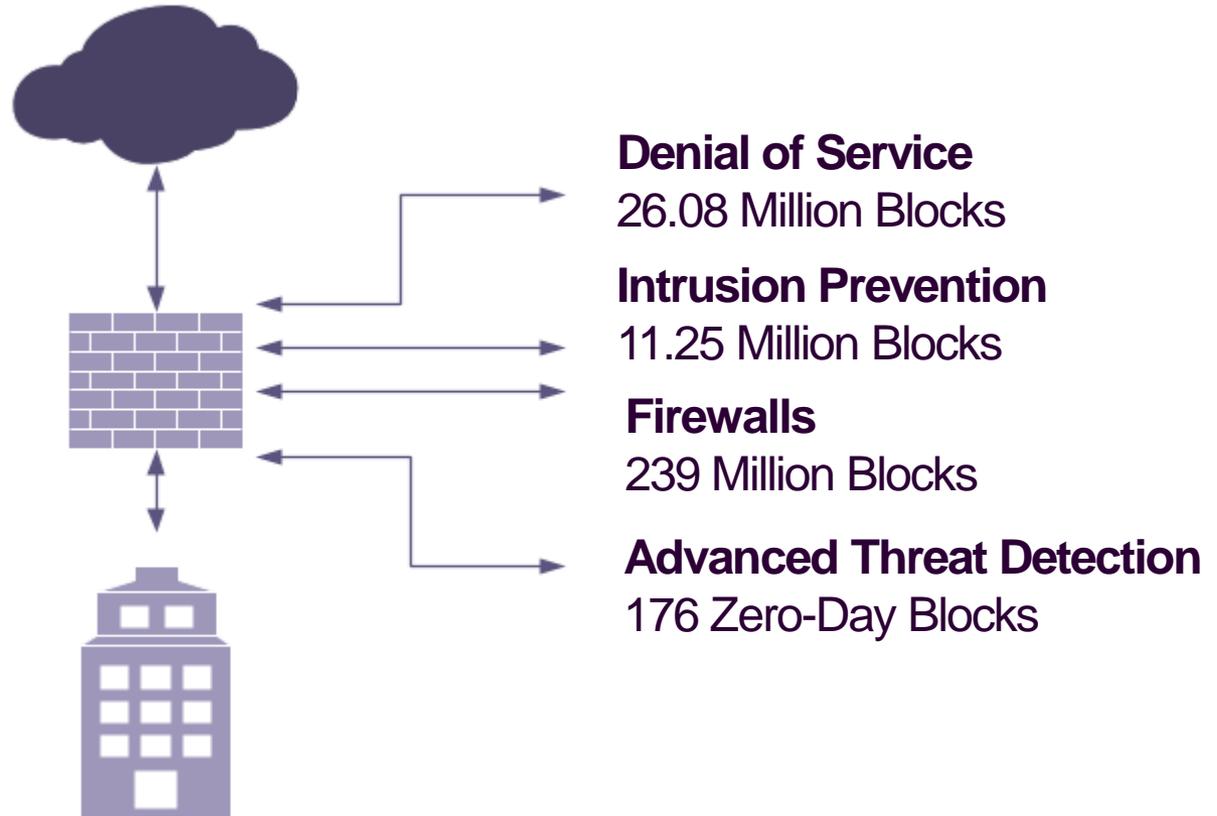


Categories

	 Personnel	 Systems	 Services
Solutions	<ul style="list-style-type: none"> • Awareness materials • Training • Shared Knowledge 	<ul style="list-style-type: none"> • Threat Intelligence • Common Operational Picture 	<ul style="list-style-type: none"> • Network Monitoring • Malware Analysis • Digital Forensics

Defense in Depth

Week of January 15 – January 21



Defense in Depth

Week of January 15 – January 21

Security Operations Center

- 26 Alerts
 - Malicious Software (17)
 - Investigations (5)
 - Account Compromise (4)



Response Team

- 2 Response Incidents

Digital Forensics

- 2 Cases

What is an Exploit Kit?

Malicious software package to automate the exploitation of a target's vulnerabilities

Key characteristics:

- Designed for Novices
- Simple User Interface
- Packages Multiple Attacks
- Tech Support
- Performance Metrics

The screenshot shows the Blackhole exploit kit control panel. The interface is in Russian and features a dark navigation bar at the top with tabs for 'СТАТИСТИКА' (Statistics), 'ПОТОКИ' (Streams), 'ФАЙЛЫ' (Files), 'БЕЗОПАСНОСТЬ' (Security), and 'НАСТРОЙКИ' (Settings). The main content area is divided into several sections:

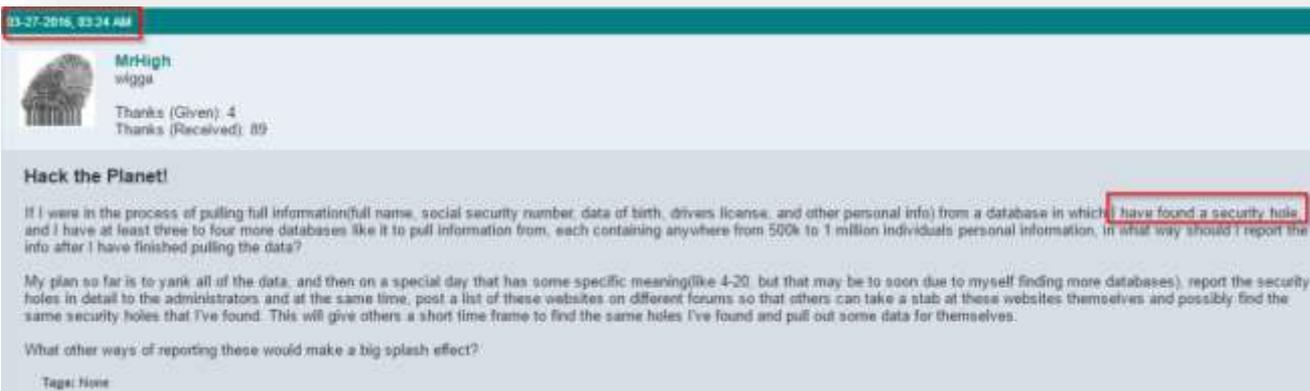
- ИЗМЕНЕНИЕ ИМЕНИ СКРИПТА** (Script Name Change): Fields for 'Имя главного скрипта:' (admin), 'Имя скрипта публичной статистики:' (stats), 'Имя скрипта входящего трафика:' (index), and 'Имя параметра потока:' (threadID), each with an 'Изменить' (Change) button.
- ИЗМЕНИТЬ ПАРОЛЬ** (Change Password): Fields for 'Старый пароль:' (Old password), 'Новый пароль:' (New password), and 'Подтвердите пароль:' (Confirm password), with an 'Изменить пароля' (Change password) button.
- ИЗМЕНИТЬ ИНТЕРВАЛ ОБНОВЛЕНИЯ** (Change Update Interval): A slider ranging from 'never' to '10 min', currently set to '5 сек.', with an 'Изменить: 5 сек.' (Change: 5 sec.) button.
- ИНТЕРФЕЙС** (Interface): Dropdowns for 'Язык:' (Russian) and 'Шаблон:' (default), each with an 'Изменить' (Change) button.
- ЛИМИТЫ** (Limits): Input fields for 'Лимит браузеров:' (10), 'Лимит ОС:' (10), 'Лимит стран:' (15), and 'Лимит рефереров:' (10). A checkbox 'Вести учет рефереров' (Track referrers) is checked. A 'Сохранить' (Save) button is present.
- VIRTEST**: Fields for 'Логин:' (userlogin) and 'Пароль:' (password), with a 'Сохранить' (Save) button.
- УДАЛЕНИЕ СТАТИСТИКИ** (Delete Statistics): A red 'Удалить все' (Delete all) button. A warning message: 'Вы не сможете восстановить данные после удаления, будьте внимательны' (You cannot restore data after deletion, be careful). A dropdown for 'Поток:' (default) with a red 'Удалить' (Delete) button.

Zero Day Detections – Past 6 Months

Events	 Unique Hosts	 Malware
5	5	Exploit.Angler
7779	4258	Exploit.HTML.IframeRef.A
2836	1893	Exploit.Kit.Angler
112	60	Exploit.Kit.Clickfraud
7	7	Exploit.Kit.Flash
2	1	Exploit.Kit.Magnitude
30	27	Exploit.Kit.Malvertiseme
59	48	Exploit.Kit.Neutrino
32	28	Exploit.Kit.Nuclear
715	162	Exploit.Kit.Redirect
563	65	Exploit.Kit.Rig
2	1	Exploit.Kit.Sundown
38	12	Exploit.Kit.TDS
732	164	Local.Infection
938	208	Malicious.URL
3	2	Trojan.Ramnit

Case Study: Fish and Wildlife

- ▶ Petty criminal cyber actor: “MrHigh”
- ▶ Self reported
- ▶ Multiple states impacted: WA, OR, ID
 - ▶ WA: 2,435,452 records (Last 4 of SSN #)
 - ▶ OR: 1,195,204 records
 - ▶ ID: 788,064 records (Full SSN #)



Case Study: Spear Phishing

- ▶ Sophisticated cyber actor
- ▶ Multiple accounts impacted



Summary

- Security is empowered by relationships
- Attack tools, techniques, and procedures evolve as defense strengthens
- Proper defenses require intelligence about the adversaries
- The State of Washington is considered a leader amongst its peers

Questions?