# Threat Hunting
# Проактивное обнаружение современных киберугроз

Вадим Хрыков, BI.ZONE SOC

# Whoami

- Руководитель отдела реагирования на инциденты, BI.ZONE SOC
- Threat Hunter
- Фанат ELK и Velociraptor
- Ex- разработчик .NET/MSSQL
- Ex- AppSec специалист
- OSCP, GIAC GCDA, CRTE
- Twitter @BlackMatter23

# FireEye M-Trends 2020

**Dwell time** – кол-во дней с момента компрометации сети до обнаружения угрозы

**GLOBAL MEDIAN DWELL TIME BY YEAR**

| Compromise Notifications | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|
| All | 416 | 243 | 229 | 205 | 146 | 99 | 101 | 78 | 56 |
| Internal Detection | — | — | — | — | 56 | 80 | 57.5 | 50.5 | 30 |
| External Notification | — | — | — | — | 320 | 107 | 186 | 184 | 141 |

# В чем причина?

- Фокус на **предотвращении** атак, а не на их обнаружении
- “Нас точно не взломают, мы надежно защищены”
- Плохое знание своей инфраструктуры
- Отсутствие квалифицированных специалистов
- “Мы купили SIEM и собираем события – SOC построен”
- Alert-driven мониторинг
- Угрозы эволюционируют быстрее

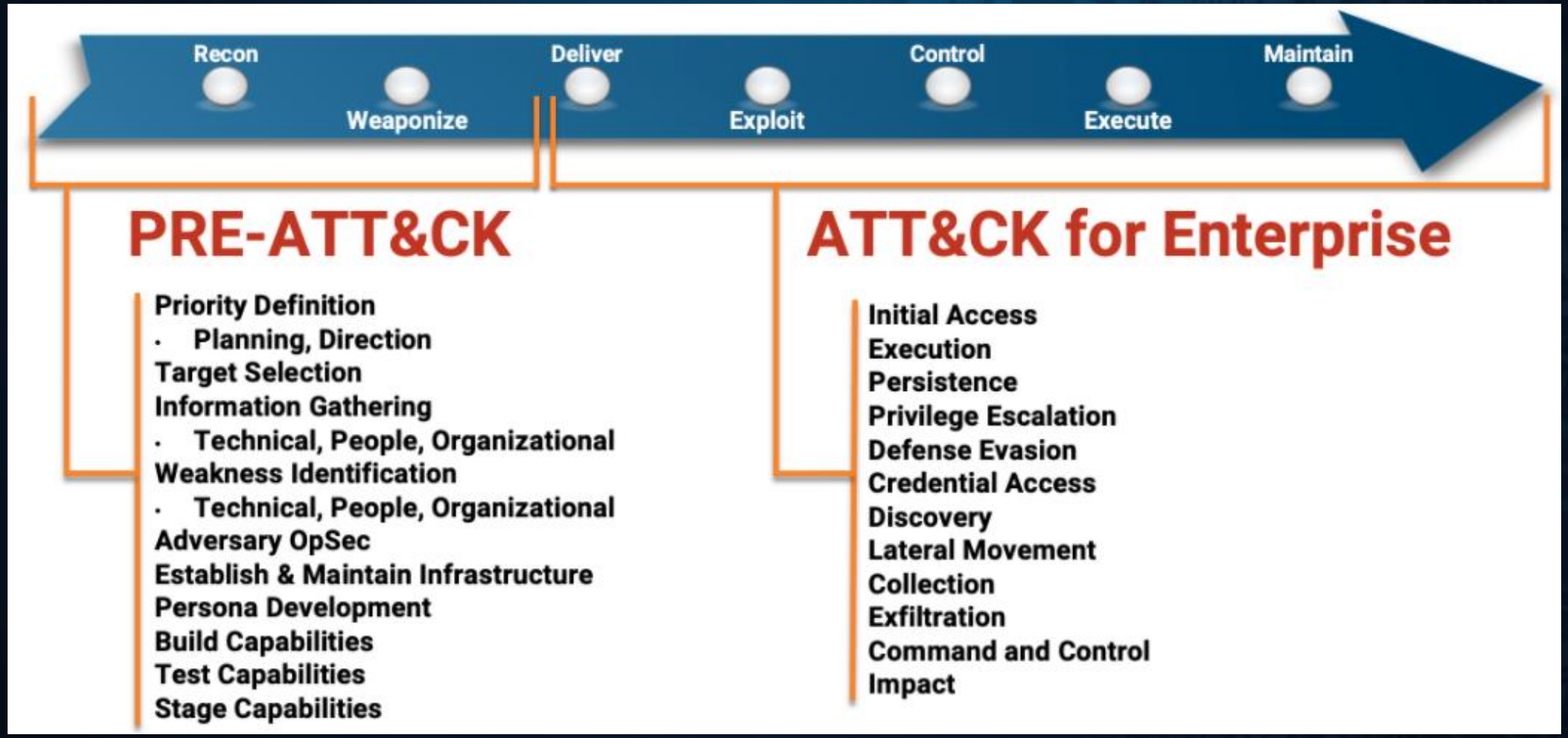
# Появление Threat Hunting

- Ответ защитников в гонке вооружений
- 2011г. - Richard Bejtlich использует термин «hunter-killer»
- Упражнения по охоте на атакующих (ВВС США)
- Начало формирования как отдельной дисциплины ИБ
- Драйверы развития:
  - Threat Intelligence (кибербразведка)
  - Endpoint Detection & Response (EDR)

# Столпы Threat Hunting

- «Prevention is Ideal, but Detection **is a Must**»
- Проактивный поиск киберугроз
- Принцип «Assume Breach»
- Прервать Kill Chain атакующего – тоже победа
- Intelligence-driven Detection & Response
- Знание TTPs атакующих (MITRE ATT&CK)
- Mindset атакующего

# Немного терминов – Cyber Kill Chain

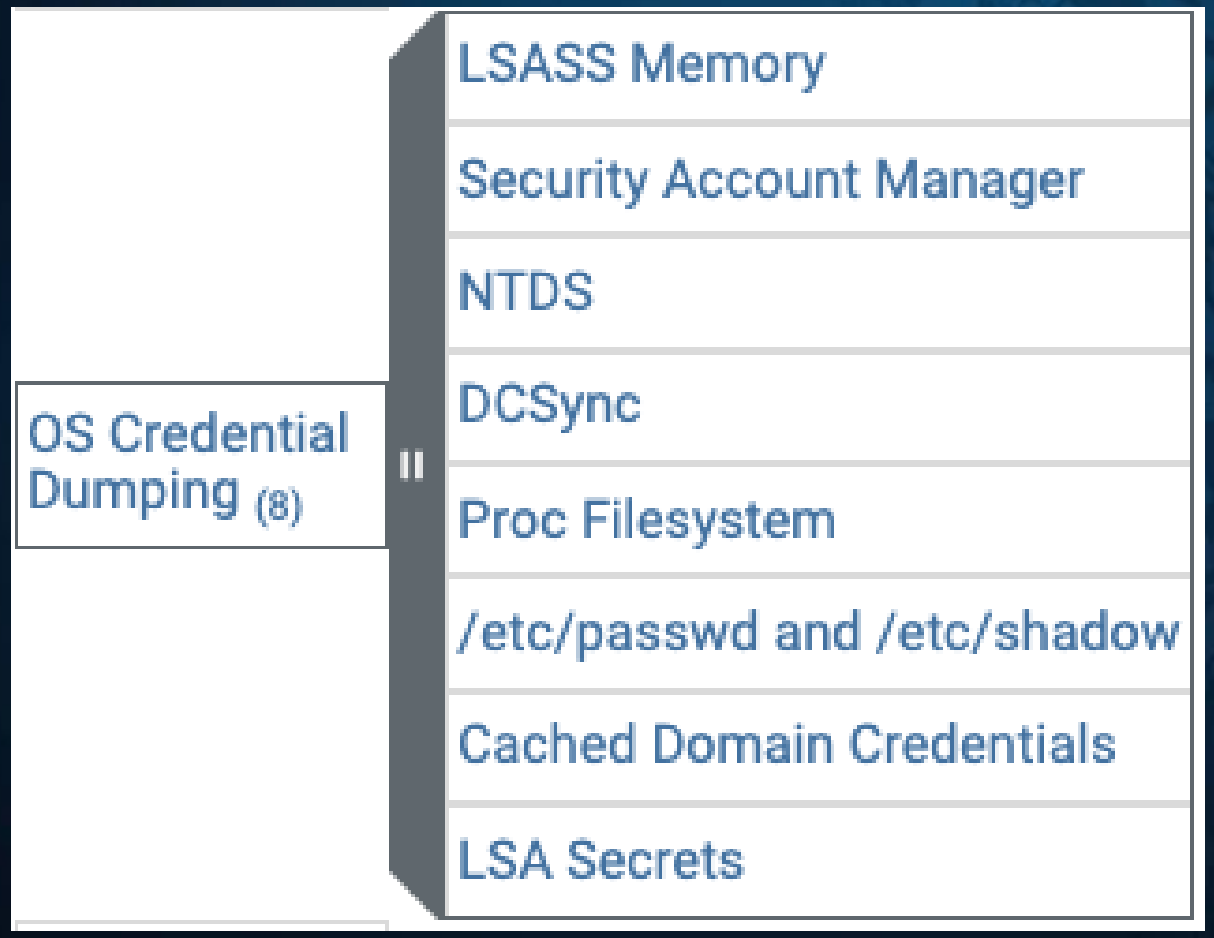


# Матрица MITRE ATT&CK

## ATT&CK Matrix for Enterprise

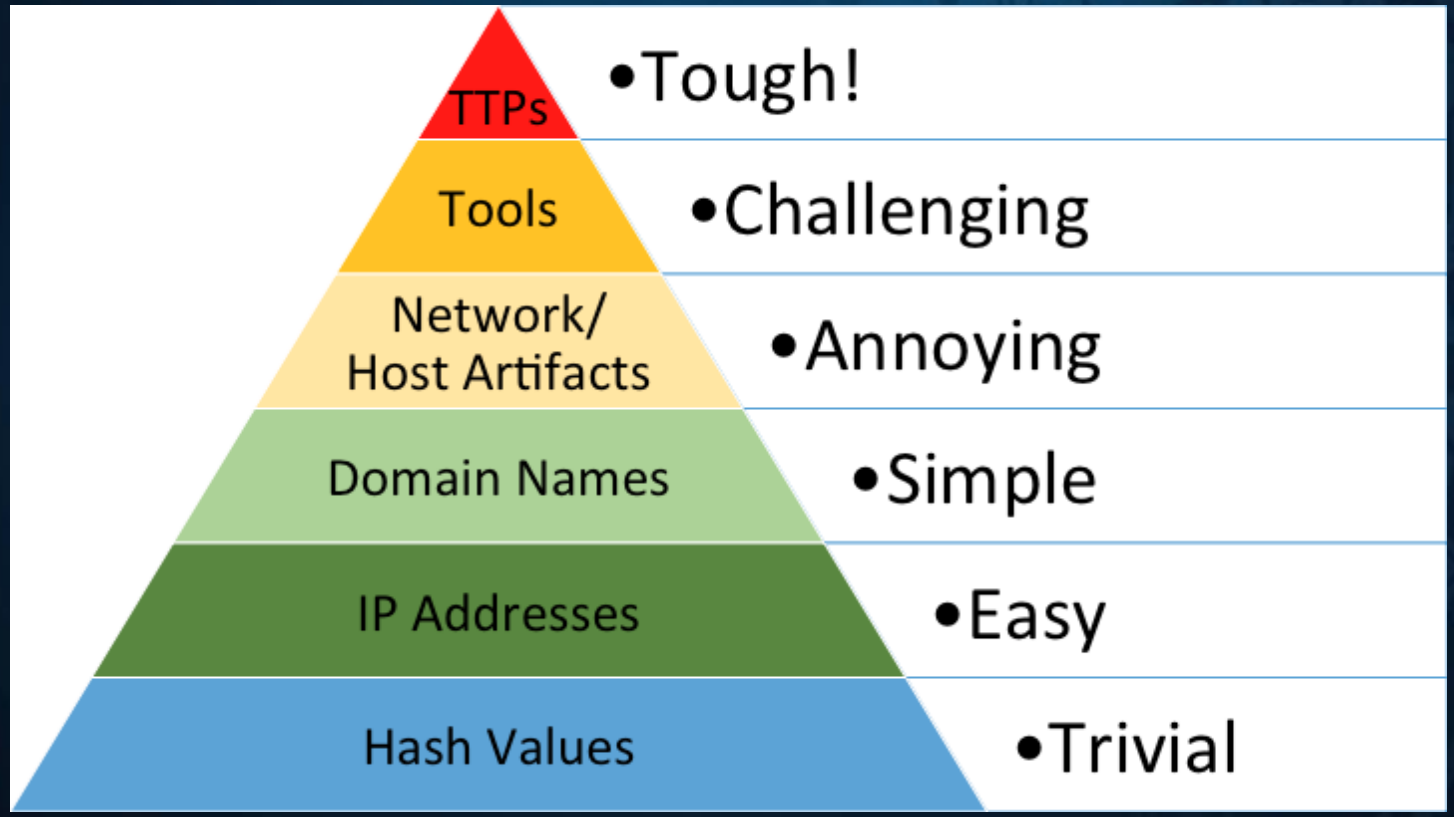
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Account Access Removal |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | Binary Padding | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Communication Through Removable Media | Data Compressed | Data Destruction |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Component Object Model and Distributed COM | Clipboard Data | Connection Proxy | Data Encrypted | Data Encrypted for Impact |
| Hardware Additions | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | Domain Trust Discovery | Exploitation of Remote Services | Data from Information Repositories | Custom Command and Control Protocol | Data Transfer Size Limits | Defacement |
| Replication Through Removable Media | Component Object Model and Distributed COM | AppInit DLLs | Application Shimming | Clear Command History | Credentials from Web Browsers | File and Directory Discovery | Internal Spearphishing | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol | Disk Content Wipe |
| Spearphishing Attachment | Control Panel Items | Application Shimming | Bypass User Account Control | CMSTP | Credentials in Files | Network Service Scanning | Logon Scripts | Data from Network Shared Drive | Data Encoding | Exfiltration Over Command and Control Channel | Disk Structure Wipe |
| Spearphishing Link | Dynamic Data Exchange | Authentication Package | DLL Search Order Hijacking | Code Signing | Credentials in Registry | Network Share Discovery | Pass the Hash | Data from Removable Media | Data Obfuscation | Exfiltration Over Other Network Medium | Endpoint Denial of Service |
| Spearphishing via Service | Execution through API | BITS Jobs | Dylib Hijacking | Compile After Delivery | Exploitation for Credential Access | Network Sniffing | Pass the Ticket | Data Staged | Domain Fronting | Exfiltration Over Physical Medium | Firmware Corruption |
| Supply Chain Compromise | Execution through Module Load | Bootkit | Elevated Execution with Prompt | Compiled HTML File | Forced Authentication | Password Policy Discovery | Remote Desktop Protocol | Email Collection | Domain Generation Algorithms | Scheduled Transfer | Inhibit System Recovery |
| Trusted Relationship | Exploitation for Client Execution | Browser Extensions | Emond | Component Firmware | Hooking | Peripheral Device Discovery | Remote File Copy | Input Capture | Fallback Channels | | Network Denial of Service |
| Valid Accounts | Graphical User Interface | Change Default File Association | Exploitation for Privilege Escalation | Component Object Model Hijacking | Input Capture | Permission Groups Discovery | Remote Services | Man in the Browser | Multi-hop Proxy | | Resource Hijacking |
| | InstallUtil | Component Firmware | Extra Window Memory Injection | Connection Proxy | Input Prompt | Process Discovery | Replication Through Removable Media | Screen Capture | Multi-Stage Channels | | Runtime Data Manipulation |

# Тактика Credential Access



# Pyramid of Pain

David J Bianco 2013r.

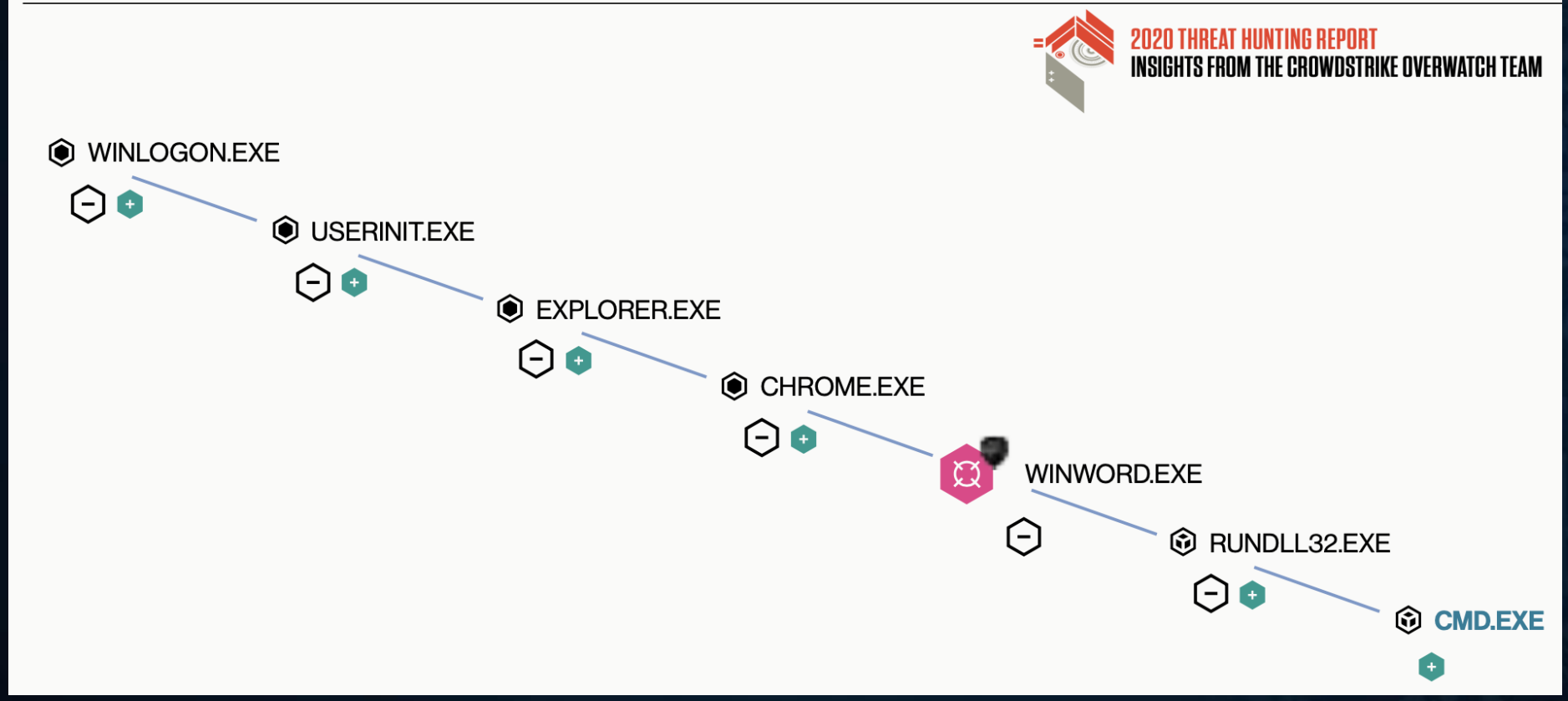


# Что нужно для Threat Hunting?

- **Команда**
  - глубокие знания безопасности ОС и сетей
  - внутренние механизмы ОС
  - киберразведка
  - хостовая и сетевая форензика
  - реагирование на инциденты
- **Данные**
  - штатные события ОС
  - расширенная телеметрия EDR
  - сетевая телеметрия
- **Инструменты**
- **Процессы**

# Умение находить аномалии

**Figure 13: Example process tree of a `cmd.exe` shell spawned under the suspicious `rundll32.exe` process**



# Охота на Impacket

- **IoC-based** подход
- хэш-суммы некоторых утилит из состава Impacket

| Tools | MD5 | SHA1 |
|---|---|---|
| psexec.py | 2773C4094DACED9F193C3B310B6CC287 | 1CB2D13297C7A82DEF2A8408CEAB05FD9A25A5CA |
| smbexec.py | DC8094A0E2A5AA30677C4D6B31523356 | A6265D68F7AB1FACED6B0652E2D4C189AD0DE2B8 |
| wmiexec.py | 15CF3D5B72D037EAE9D1CE18F9179B4B | 81D9A370D3C1C64E1F9C0DCDABBB241A7C1EF20F |

# Охота на Impacket

- **Tools-based** подход (Smbexec.py)

| Host Indicators | Network Indicators |
| --- | --- |
| Process-specific command lines:<br><br>C:\Windows\system32\cmd.exe /Q /c echo cd ^> \\127.0.0.1\C$__output 2^>^&1 ><br><br>C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c<br><br>C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat | A specific name of a remotely created service:<br><br>content: “B\|00\|T\|00\|O\|00\|B\|00\|T\|00\|O”<br><br>A specific command line for the created service (lpBinaryPathName):<br><br>content: “%\|00\|C\|00\|O\|00\|M\|00\|S\|00\|P\|00\|E\|00\|C\|00\|%\|00\| \|00\|/\|00\|Q\|00\| \|00\|/\|00\|c\|00\| \|00\|e\|00\|c\|00\|h\|00\|o\|00\| ”;<br><br>A specific host name used as an argument of function ROpenSCManager:<br><br>content: “D\|00\|U\|00\|M\|00\|M\|00\|Y” |

# Охота на Impacket

- **TTPs-based** подход
- *PsExec использует протокол SMB для подключения к удаленному хосту, копирует файл с полезной нагрузкой, создает сервис с «рандомным» именем и запускает скопированный файл*

- Идеи для детектирующих правил:
  - сетевой вход на хост с последующим созданием в системе сервиса;
  - создание и удаление сервиса в короткий промежуток времени;
  - создание сервиса с «рандомным» именем;
- Практические любые “ханты” могут выдавать FPs
- Для корректировки правил нужно много телеметрии
- SIGMA правила требуют много тюнинга

# Генерация идей для гипотез

- Техники матрицы MITRE ATT&CK
- Анализ отчетов Threat Intelligence
- Блоги, Твиттер, доклады на конференциях
- CTFs, Virtual Labs (HTB, GCB, OffSec PG и т.д.)
- Практики реагирования на инциденты
- Практики тестирования на проникновение
- Курсы по практической кибербезопасности

# TTPs - Labyrinth Chollima (КНДР)


- Цитаты из отчета:
  - *«A suspicious dynamic link library (DLL) file named desktop.dat, masquerading as a .dat file, was loaded into memory by rundll32.exe in an unusual manner»*
  - *«Rundll32.exe was executed under Microsoft Word process»*
  - *«Example process tree of a cmd.exe shell spawned under the suspicious rundll32.exe process»*

- Идеи для гипотез:
  - создание файла с PE заголовком и нетипичным для исполняемых файлов расширением
  - старт процесса rundll32.exe родительским процессом MS Office
  - запуск командного интерпретатора cmd.exe процессом rundll32

# TTPs - PANDA (Китай)


- Цитаты из отчета:
  - *«China Chopper web shell beneath the likely exploited Apache web server process httpd.exe»*
  - *«The binary was masquerading as the Microsoft shared service host process svchost.exe»*
  - *«the actor attempted to launch PowerShell to download malicious binary»*

- Идеи для гипотез:
  - старт процессом веб-сервера командного интерпретатора cmd.exe
  - создание исполняемого скрипта в каталоге веб-сервера (по расширению)
  - создание файла веб-шелла в каталоге веб-сервера (Yara)
  - старт процесса svchost.exe из нетипичного каталога/нетипичным родителем
  - использование специфичных Powershell командлетов для скачивания файлов с внешних ресурсов

# TTPs - Tracer Kitten (Иран)


- Цитаты из отчета:
  - *«SSH tool called Bitvise was installed on the system, and proceeded to take a copy of this and rename it within an Adobe directory to appear associated with the Adobe program»*
  - *«identified that DNS (TXT record) tunneling was coded in as the C2 mechanism*
  - «atypical living-off-the-land technique being employed to exploit the LSASS process via the use of comsvc.dll*»*
  - *«the adversary attempted to run Invoke-TheHash, an application used to perform pass-the-hash attacks»*

- Идеи для гипотез:
  - запуск переименованных утилит класса RAT (VERSION INFO)
  - аномально большое кол-во DNS TXT запросов
  - запуск rundll32 с командной строкой, содержащей comsvc.dll и «MiniDump»
  - детектирование специфичных командлетов Invoke-TheHash

# Полезные ссылки

Статьи команды BI.ZONE SOC:

- **Threat Hunting. Why might you need it**
- (https://cyberpolygon.com/ru/materials/threat-hunting-in-action/)

- **Threat Hunting в действии**
- (https://cyberpolygon.com/ru/materials/threat-hunting-in-action/)

- **Threat Hunting. Охота на продвинутые тактики и техники атакующих**
- (https://cyberpolygon.com/ru/materials/hunting-for-advanced-tactics-techniques-and-procedures-ttps/)

Спасибо за внимание!