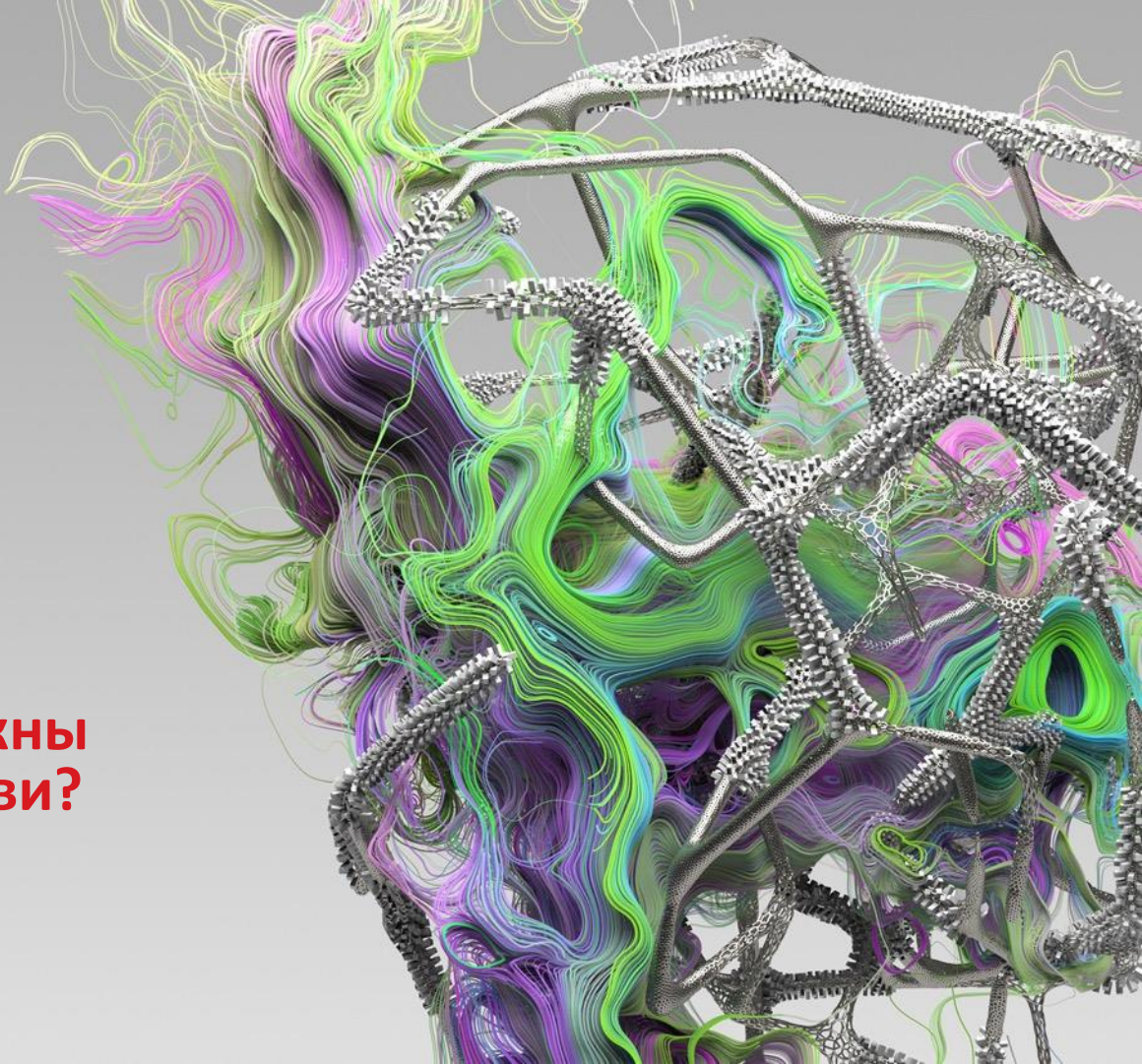




# “Если б я был султан... какие инструменты нужны для плодотворной любви?”

—  
Михаил Кондрашин  
Алматы, 8 ноября 2019



# Оглавление

- **От EDR к XDR**  
EDR, а что дальше?
- **MITRE ATT&CK**  
Как разобраться во всех хакерских приемах и технологиях
- **DEMO**  
Как выглядит XDR
- **MXDR**  
Это вообще что?

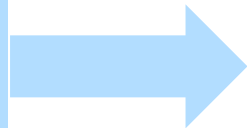






# Обнаружение и реакция на конечной точке (EDR)

Детекты  
Телеметрия  
Метаданные



Протоколирование  
всей активности на  
рабочей станции



Автоматическая  
корреляция и  
обнаружение



Прочесывание  
по индикаторам  
ИОС



Поиск угроз



Поиск  
первопричины

Обнаружение  
угроз

Блокировка  
угроз

Расследование  
угроз

# EDR необходим, но недостаточен



Почта



Сеть



Бессерверные  
вычисления

Требуется:  
Обнаружение и  
реакция за пределами  
рабочей станции



Конечные  
точки



Сервера и облачные  
вычислительные  
МОЩНОСТИ



IoT



Контейнеры

Сегодня

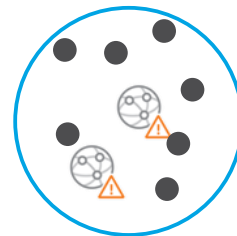
# Угрозы избегают обнаружения, потому, что данные собираются и анализируются по отдельности

Рабочие  
станции



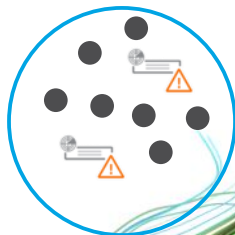
IoT

Почта



Сеть

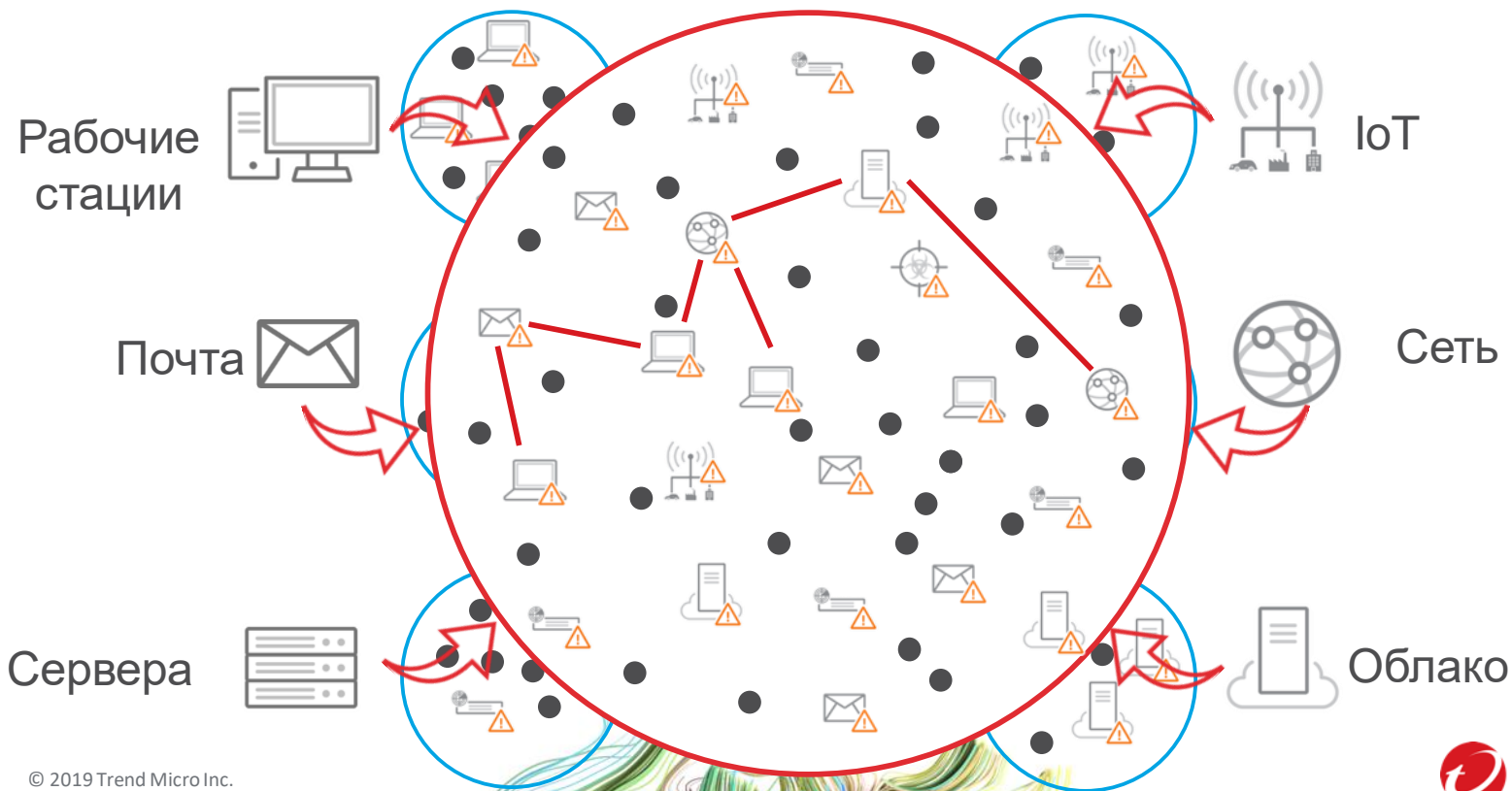
Сервера



Облако

Требуется

# Корреляция и аналитика сквозь все эшелоны защиты





## Корреляция и аналитика сквозь все эшелоны защиты



# Trend Micro XDR

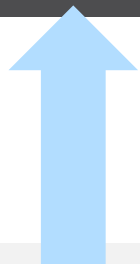
## Услуги Trend Micro Managed XDR

### Trend Micro XDR

*Автоматическое обнаружение, Прочесывание, Поиск, Анализ первопричины*

«Озеро» данных Trend Micro XDR

Активность  
&  
обнаружения



**Сеть**



Deep Discovery, TippingPoint



**Пользователи**



**Email**

Cloud App Security



**Endpoint**

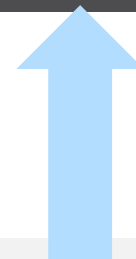
Apex One



**Облака**



Deep Security

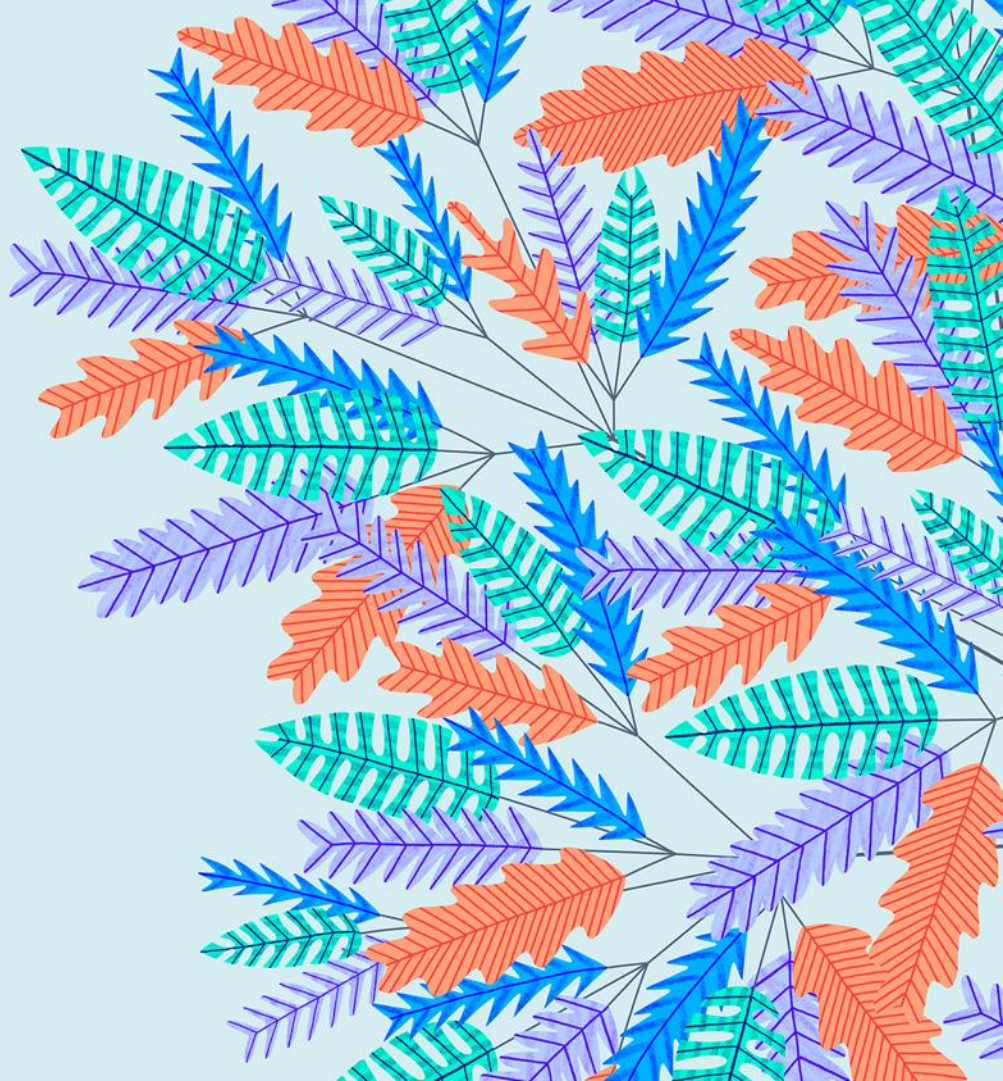


**Будущее**



# MITRE ATT&CK

—



# Что такое MITRE ATT&CK на самом деле?

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command And Control
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items	19 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	Credential Dumping	File and Directory Discovery	Dynamic Data Exchange	Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Command History	Credentials in Files	Exploitation of Vulnerability	Distributed Component Object Model	Execution through API	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signing	Exploitation of Vulnerability	Network Service Scanning	Exploitation of Vulnerability	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Forced Authentication	Network Share Discovery	Logon Scripts	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Bootkit	Component Object Model Hijacking	Deobfuscate/Decode Files or Information	Hooking	Peripheral Device Discovery	Pass the Hash	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Browser Extensions	DLL Search Order Hijacking	Disabling Security Tools	Input Prompt	Query Registry	Pass the Ticket	Launchctl	Data from Removable Media	Exfiltration Over Other Network Medium	Domain Fronting
Change Default File Association	Dylib Hijacking	DLL Search Order Hijacking	Keychain	Process Discovery	Remote Desktop Protocol	Local Job Scheduling	Data Staged	Exfiltration Over Physical Medium	Fallback Channels
Component Firmware	Exploitation of Vulnerability	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Query Registry	Remote Services	LSASS Driver	Email Collection	Exfiltration Over Physical Medium	Multi-hop Proxy
Component Object Model Hijacking	Extra Window Memory Injection	Exploitation of Vulnerability	Network Sniffing	Remote System Discovery	Replication Through Removable Media	Mshta	Input Capture	Scheduled Transfer	Multi-Stage Channels
Create Account	File System Permissions Weakness	Extra Window Memory Injection	Password Filter DLL	Security Software Discovery	Shared Webroot	PowerShell	Man in the Browser	Screen Capture	Multiband Communication
DLL Search Order Hijacking	Hooking	File System Logical Offsets	Private Keys	System Information Discovery	SSH Hijacking	Regsvcs/Regasm	Screen Capture	Video Capture	Multilayer Encryption
Dylib Hijacking	Image File Execution Options Injection	Gatekeeper Bypass	Replication Through Removable Media	System Network Configuration Discovery	Taint Shared Content	Regsvr32	Remote File Copy		Remote File Copy
External Remote Services	Launch Daemon	Hidden Files and Directories	Securityd Memory	System Network Connections Discovery	Third-party Software	Rundll32	Standard Application Layer Protocol		Standard Application Layer Protocol
File System Permissions Weakness	Hidden Files and Directories	Hidden Users	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Scheduled Task	Standard Cryptographic Protocol		Standard Cryptographic Protocol
Hidden Files and Directories	New Service	Hidden Window		System Owner/User Discovery	Windows Remote Management	Scripting	Standard Non-Application Layer Protocol		Standard Non-Application Layer Protocol
Hooking	Path Interception	HISTCONTROL		System Service Discovery		Service Execution	Uncommonly Used Port		Uncommonly Used Port
Hypervisor	Plist Modification	Image File Execution Options Injection		System Time Discovery		Source	Web Service		Web Service
Image File Execution Options Injection	Port Monitors	Indicator Blocking				Space after Filename			
Launch Agent	Process Injection	Indicator Removal from Tools				Third-party Software			
Launch Daemon	Scheduled Task	Indicator Removal on Host				Trap			
Launchctl	Service Registry Permissions Weakness	Install Root Certificate				Trusted Developer Utilities			
LC_LOAD_DYLIB Addition	Setuid and Setgid	InstallUtil				Windows Management Instrumentation			
Local Job Scheduling	SID-History Injection					Windows Remote Management			

# Пример: APT28

**Описание:** APT28 чаще всего атрибутируют связью с РФ

---

**Псевдонимы:** Sednit, PawnStrom, FancyBear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

---

**Технические приемы:**

- Обфускация данных
- Проксирование соединений
- Использование стандартных протоколов
- Удаленное копирование файлов
- Rundll32
- Удаление индикатора на хосте
- Подмена времени модификации файла
- Кража реквизитов
- Захват экрана
- Модификация MBR

---

**Программы:** Chopstick, JHUHUGIT, ADVSTORESHELL, Xtunnel, Mimikatz, HIDE DRV, USBStealer, CORESHELL, OLDBAIT, XAgentOSX, Komplex, Responder, Forfiles, Winexe, certutil

---

**Ссылки:** Fireeye. (2015) APT28:



# Пример технического приема: New Service

<b>Описание:</b>	Когда операционная система загружается, она запускает программы, которые называются «службы», которые выполняют фоновые задачи. Злоумышленники устанавливают свои службы, модифицируя системный реестр или используя утилиты командной строки
<b>Платформа:</b>	Windows
<b>Требуемый уровень доступа:</b>	Administrator, SYSTEM
<b>Итоговый уровень доступа:</b>	SYSTEM
<b>Обнаружение:</b>	Мониторинг системного реестра с целью выявления создания новых служб и утилит, запускаемых из командной строки
<b>Защита:</b>	Ограничение полномочий профилей пользователей и предотвращение повышения полномочий
<b>Источники данных:</b>	Реестр Windows, мониторинг процессов, параметры командной строки
<b>Примеры:</b>	Carbank, Lazarus Group, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, ...
<b>Ссылки:</b>	1. Microsoft. (n.d.). Services. Retrieved June 7, 2016.

# Пример программы: CHOPSTICK

---

<b>Описание:</b>	CHOPSTICK — это семейство вредоносных программ, представляющих собой модульные системы предоставления удаленного доступа, используемые группой APT28. Она была замечена в ноябре 2012 и обнаруживалась до августа 2016 года. Как правило она появлялась на компьютерах жертв, как вторая стадия атаки, но в некоторых случаях она сама была первой стадией.
<b>Псевдонимы:</b>	CHOPSTICK, SPLM, Xagent, webhp
<b>Технические приемы:</b>	Захват ввода: CHOPSTICK способен перехватывать нажатия на клавиатуре Интерфейс командной строк: CHOPSTICK способен запускать удаленные команды Резервные каналы: CHOPSTICK переключается на резервные канал связи, если основной не работает Проксирование соединений: CHOPSTICK использует прокси для коммуникации между жертвами и центром управления И многое другое...
<b>Группы:</b>	APT28
<b>Ссылки:</b>	Fireeye. (2015). APT28

---

# MITRE ATT&CK в ApexCentral

Apex Central™ mitre

Dashboard Directories Policies Threat Intel Response Detections Administration Help

Log Query

Attack Discovery Engine Information All products Last 24 hours Search Show advanced filters

Customize Columns Export to CSV Export to XML

Detection Time	Received	Host Name	Client IP	Risk Level	Rule ID	Tactics	Techniques	Count
04/19/2019 10:28:20	04/19/2019 10:30:06	I27w10x86rs5	10.201.140.219	Medium	File Permissions Modification on Accessibilit...	Defense Evasion (TA0005)	File Permissions Modification (T1222)	1
04/18/2019 16:32:02	04/18/2019 16:34:00	I27w10x86rs5	10.201.140.219	Medium	File Permissions Modification on Accessibilit...	Defense Evasion (TA0005)	File Permissions Modification (T1222)	2
04/18/2019 15:53:57	04/18/2019 15:55:01	Win7SP1x64	10.1.174.15	Low	Data compression	Exfiltration (TA0010)	Data Compressed (T1002)	2
04/18/2019 15:40:45	04/18/2019 15:46:00	Win7SP1x64	10.1.174.15	Medium	ioa_7	Lateral Movement (TA0008)	HISTCONTROL (T1148).LC_MAIN ...	2
04/18/2019 15:40:45	04/18/2019 15:46:00	Win7SP1x64	10.1.174.15	Medium	ioa_6	Discovery (TA0007)	Trusted Developer Utilities (T1127),...	2
04/18/2019 15:40:45	04/18/2019 15:46:00	Win7SP1x64	10.1.174.15	Medium	ioa_10	Command and Control (TA0011)	Exploitation for Defense Evasion (T...	2
04/18/2019 15:40:45	04/18/2019 15:46:00	Win7SP1x64	10.1.174.15	Medium	ioa_1	Execution (TA0002)	Data Encrypted (T1022).Shortcut M...	2
04/18/2019 15:40:45	04/18/2019 15:46:00	Win7SP1x64	10.1.174.15	Medium	ioa_5	Credential Access (TA0006)	Execution through API (T1106).File ...	2



# MITRE ATT&CK в Deep Discovery

win7

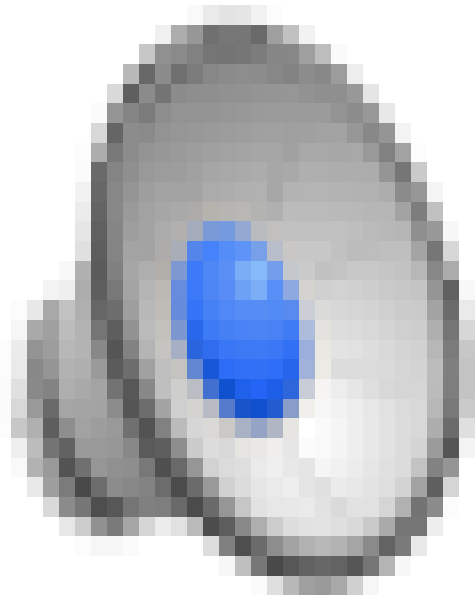
Environment-specific risk level	<b>High risk</b> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	VAN_DROPPER.UMXX, VAN_BOT.UMXX
Exploited vulnerabilities	-
Network connection	Custom

## MITRE ATT&CK Matrix

Tactic	Techniques	Notable Threat Characteristics
Execution	<a href="#">Rundll32</a>	■■■ Characteristics : 1
Persistence	<a href="#">Process Injection</a>	■■■ Characteristics : 1
Defense Evasion	<a href="#">File Deletion</a>	■■■ Characteristics : 1, 2
Discovery	<a href="#">File and Directory Discovery</a>	■■■ Characteristics : 1, 2, 3 ■■■ Characteristics: 1 ■■■ Characteristics: 1, 2
	<a href="#">Peripheral Device Discovery</a>	■■■ Characteristics : 1, 2 ■■■ Characteristics: 1
	<a href="#">Process Discovery</a>	■■■ Characteristics: 1
Collection	<a href="#">Clipboard Data</a>	■■■ Characteristics: 1


**Demo**





# Услуга Trend Micro Managed XDR

## Дополняя обнаружение и реакцию

- 
- Уведомление и мониторинг 24x7
  - Выяснение первопричины и анализ последствий
  - Расследование инцидентов и отчетность
  - Реакция и планы по восстановлению



Услуга XDR  
предоставляется  
специалистами  
Trend Micro



**Сеть**  
Deep Discovery



**Почта**  
Cloud App Security



**Рабочие станции**  
Apex One



**Сервера и облака**  
Deep Security

# Разрешение на расследование

Разрешение на

Сбор образцов файлов

Запуск инструментария для расследования

Запуск расширенной оценки угрозы

Оценка последствий

Запуск процедуры поиска первопричины

Managed Detection and Response

Pending Tasks

Task Tracking

Automated Analyses

Settings

✓ Approve

✗ Reject

	Task Description	Command	Targets	Expiration	
<input type="checkbox"/>	▶ tmik case	TMIK (Trend Micro Investigation Kit)	1	03/15/2018 18:19:26	
<input type="checkbox"/>	quick investigation case	Quick Investigation	All	03/15/2018 18:14:29	
<input type="checkbox"/>	▼ collect file case	Collect File ⓘ	6	03/15/2018 18:14:29	
	Endpoint ↕	c:\a.exe c:\b.exe	IP Address	User ▲	Endpoint Sensor Servi
<input type="checkbox"/>	Client03		100.1.1.3	✱ user03	✔ Enabled
<input type="checkbox"/>	Client01		100.1.1.1	user01	✔ Enabled
<input type="checkbox"/>	Client02		100.1.1.2 100.10.1.2 100.1.10.2 100.1.1.20	user02	✔ Enabled
<input type="checkbox"/>	Client04		100.1.1.6	user04	✘ Server license not sup
<input type="checkbox"/>	Client21		100.2.1.1	user21	✘ Disabled
<input type="checkbox"/>	Client99		N/A	N/A	✘ Agent not installed

1 - 3 / 3

< > 1 / 1 20 per page



**Спасибо!**



# THE ART OF CYBERSECURITY

Automated hybrid cloud workload protection via calls to Trend Micro APIs. Created with real data by Trend Micro threat researcher and artist **Jindrich Karasek**.