



POSITIVE
TECHNOLOGIES

Как обнаружить перемещение атакующих по сети

Егор Подмоков
Специалист PT ESC

ptsecurity.com

PT Expert Security Center



- Проводим threat hunting в инфраструктуре заказчика
- Расследуем инциденты
- Приносим экспертизу в наши продукты
- Разрабатываем правила обнаружения угроз для NTA и SIEM-систем

План вебинара

- Что такое Lateral Movement и чем он опасен
- Пример горизонтального перемещения
- Как это обнаружить в сети
- Как можно помешать распространению

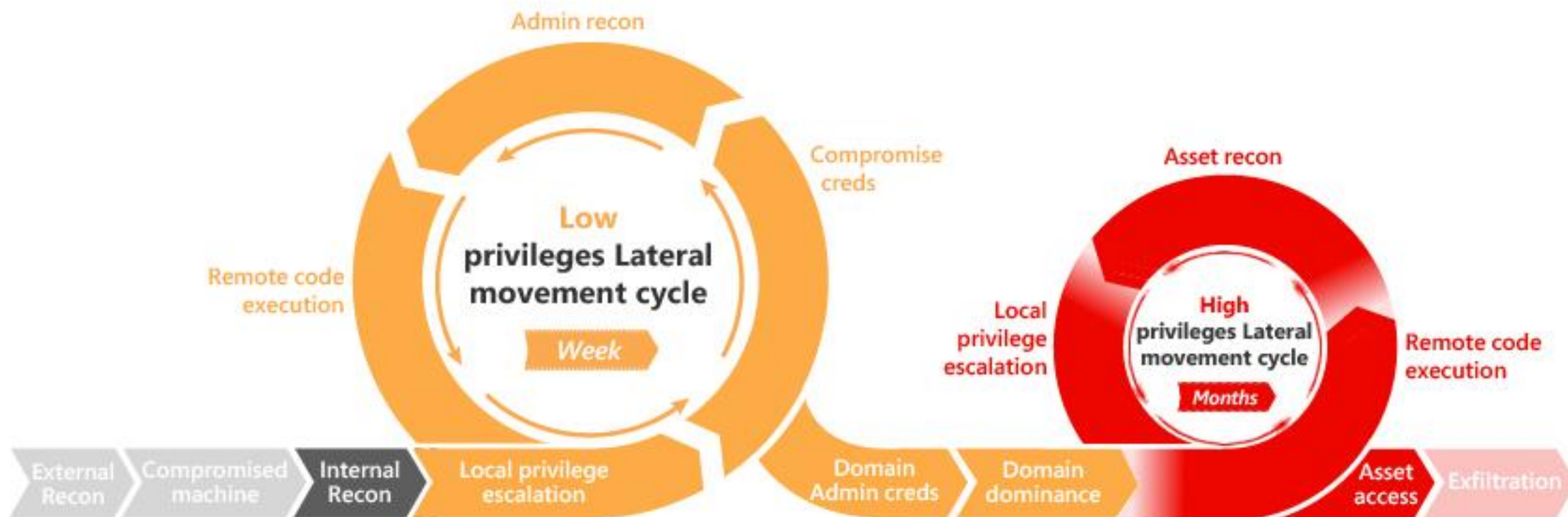
Red Team Operations Lifecycle

PT



github.com/infosecninja/Red-Teaming-Toolkit

Active Directory Kill Chain



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	Applnit 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	Applnit 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

Lateral Movement — это важно



- Нужна для развития атаки
- Изначальная компрометация может быть пропущена
- В случае успеха атакующий может завладеть учетными записями привилегированных пользователей и быстро расширить свое присутствие вплоть до полного контроля над инфраструктурой



POSITIVE
TECHNOLOGIES

Кейс перемещения атакующих по сети

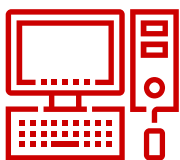


Действия злоумышленника

PT

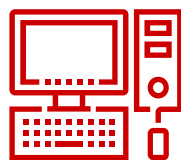
Инфраструктура

App Server



ASP server
в DMZ

DevOps



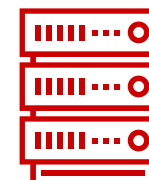
AGUSEV
contoso\agusev

HelpDesk



GPAVLOV
contoso\gpavlov
contoso\gpavlovAdm

Domain Controller



DC
contoso\Administrator

Действия злоумышленника

0. Изначальная компрометация



.Net server

Злоумышленник проломил сетевой узел и выяснил, что он является ASP (Active Server Pages) сервером для тестирования приложений.

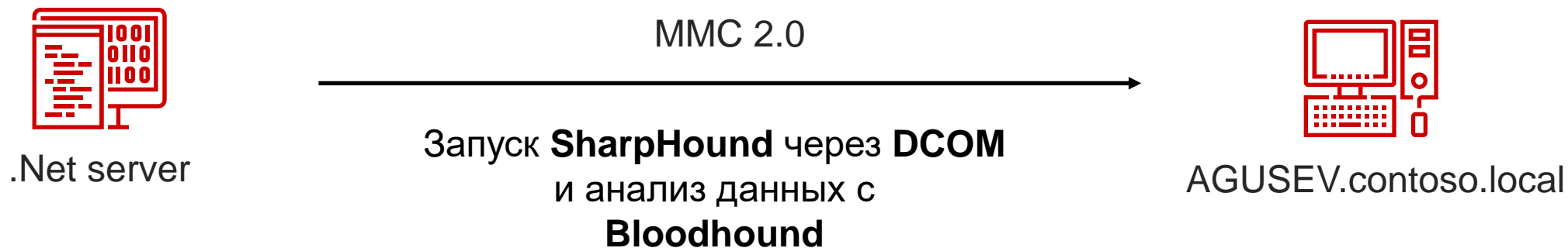
У нее есть доступ к домену, а пользователь **AGUSEV** оставил учетные данные внутри скрипта.

Почему бы и да...

Действия злоумышленника

1. Внутренняя разведка

Пользователь сервера AGUSEV уже запускал приложения для отладки через DCOM



Действия злоумышленника

1. Внутренняя разведка

DCOM (*Distributed Component Object Model*) — расширение COM для поддержки связи между объектами на различных компьютерах по сети.

COM-объект	Метод
MMC20.Application	ExecuteShellCommand()
ShellWindows	ShellExecute()
ShellBrowserWindow	ShellExecute()
Excel.ChartApplication	DDEInitiate()
...	...

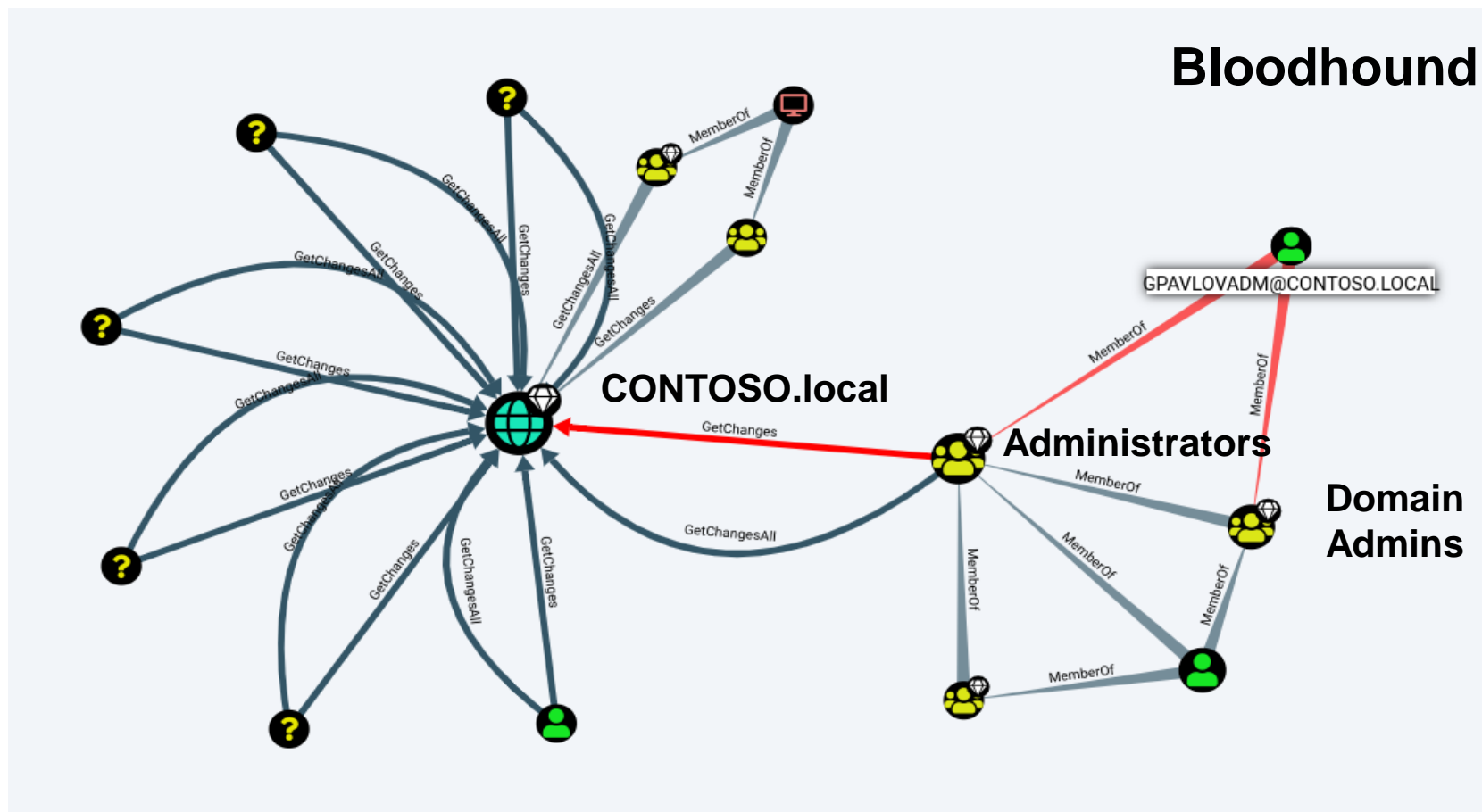
```
PS C:\Windows\system32> $mmc_o = [Activator]::CreateInstance([Type]::GetTypeFromProgID('MMC20.Application','127.0.0.1'))
PS C:\Windows\system32> $mmc_o.Document.ActiveView.ExecuteShellCommand("calc.exe", "", "", "")
PS C:\Windows\system32>
```

enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/

enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/

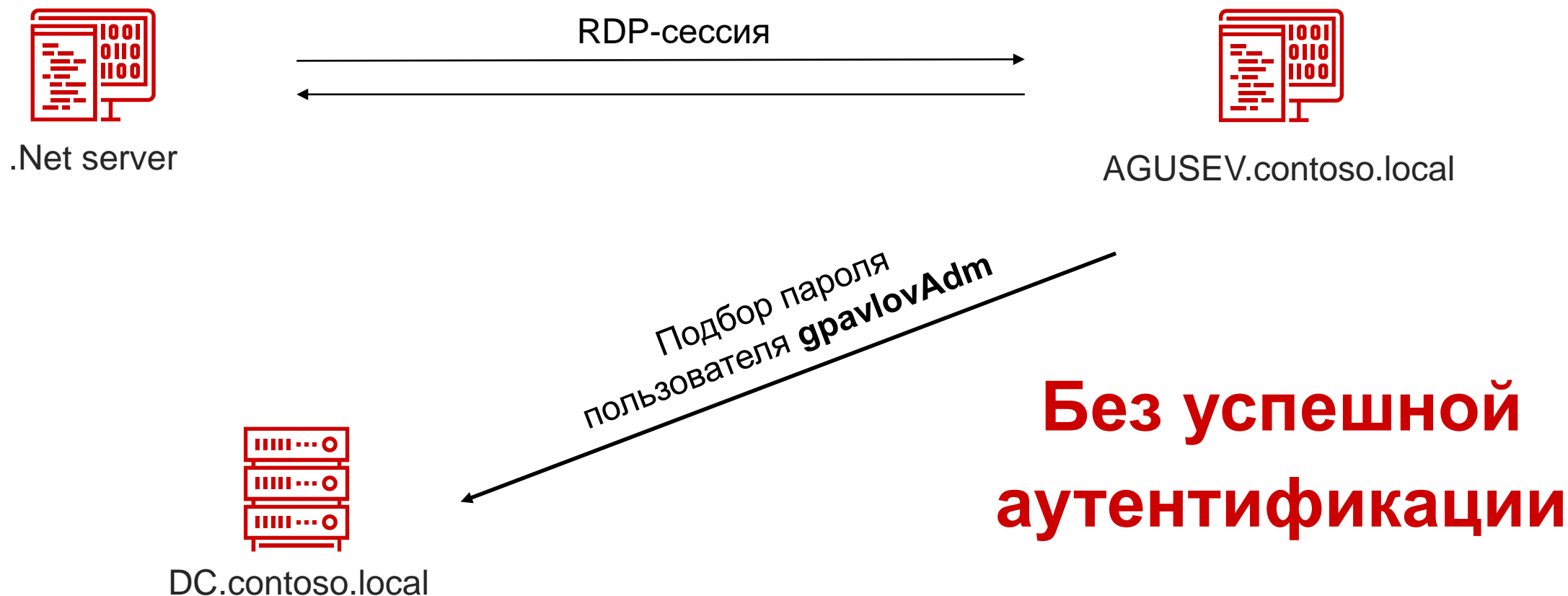
Действия злоумышленника

1. Внутренняя разведка



Действия злоумышленника

2. Подбор пароля через Kerberos

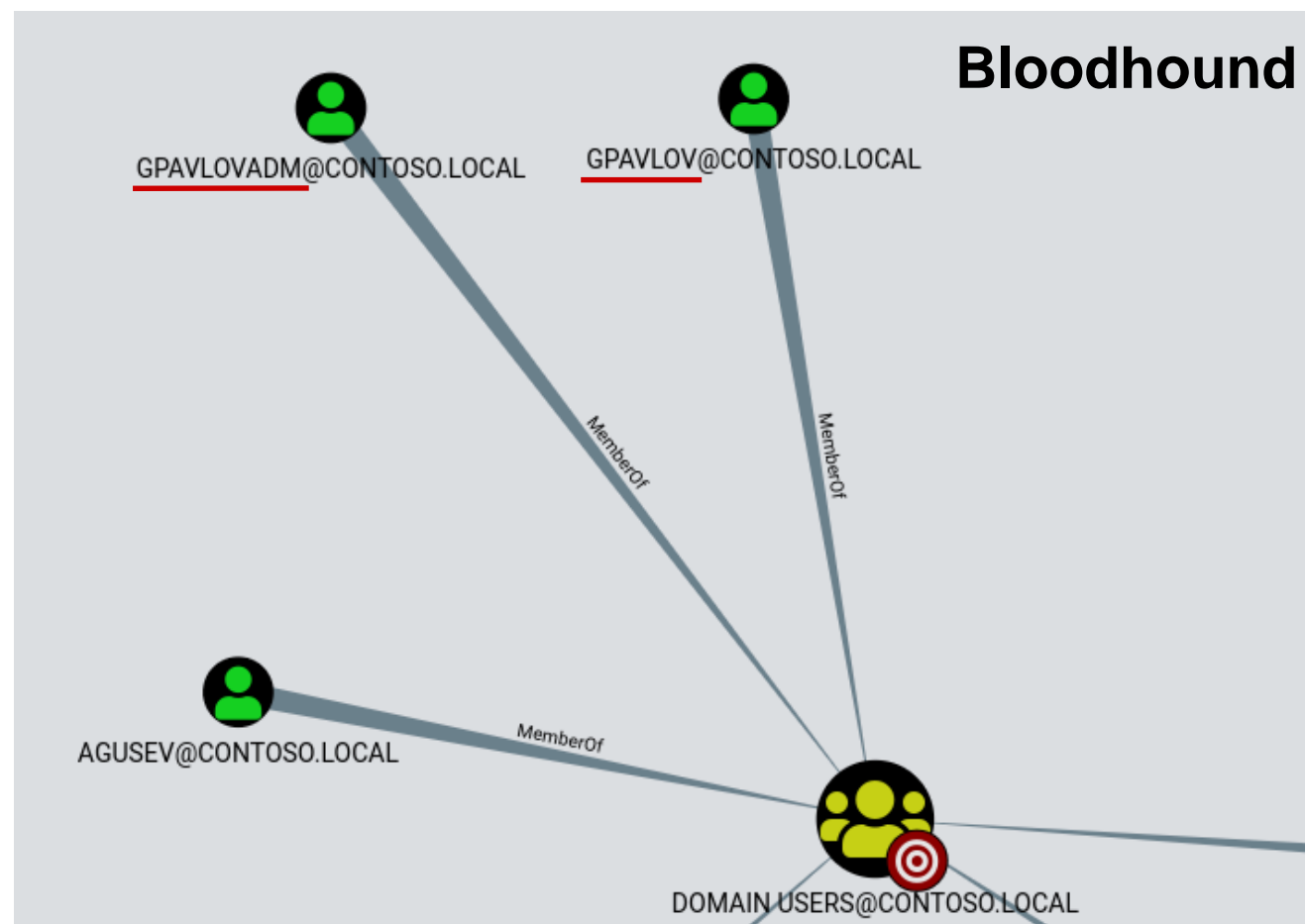


Действия злоумышленника

2. Подбор пароля через Kerberos

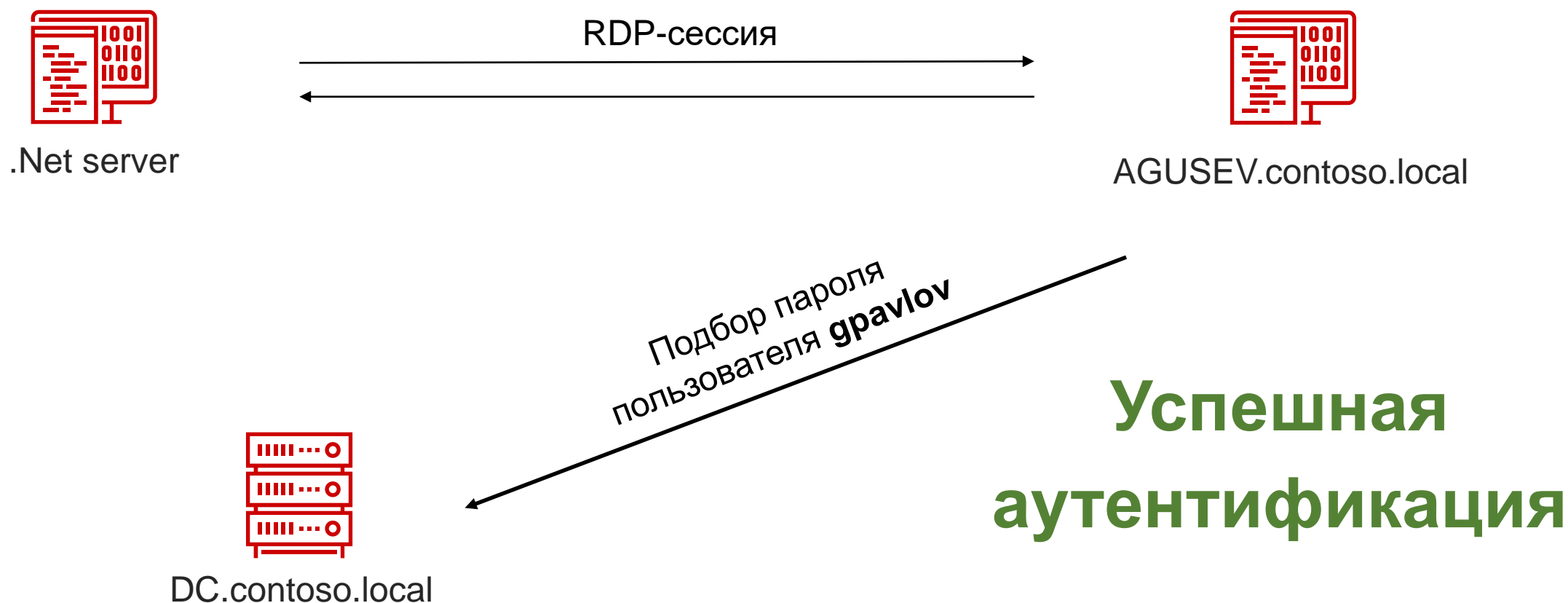
GpravlovAdm **brute fail**

Gpravlov ???



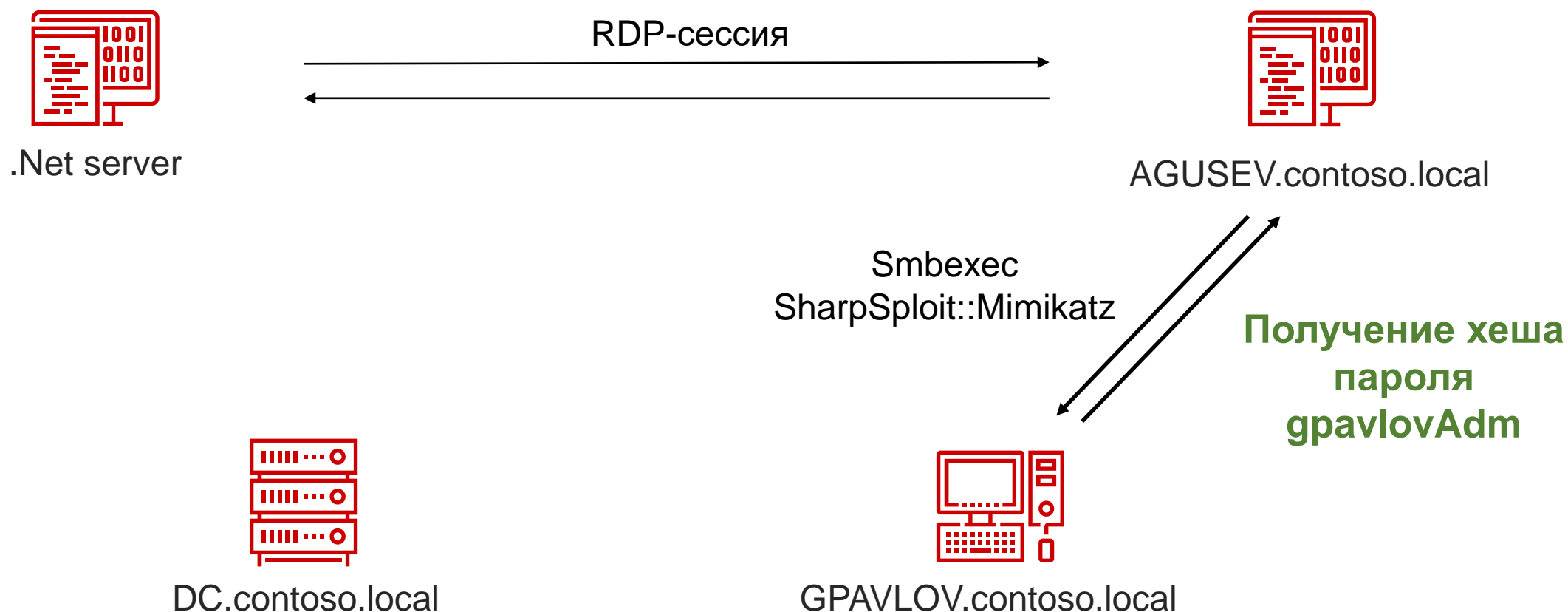
Действия злоумышленника

2. Подбор пароля через Kerberos



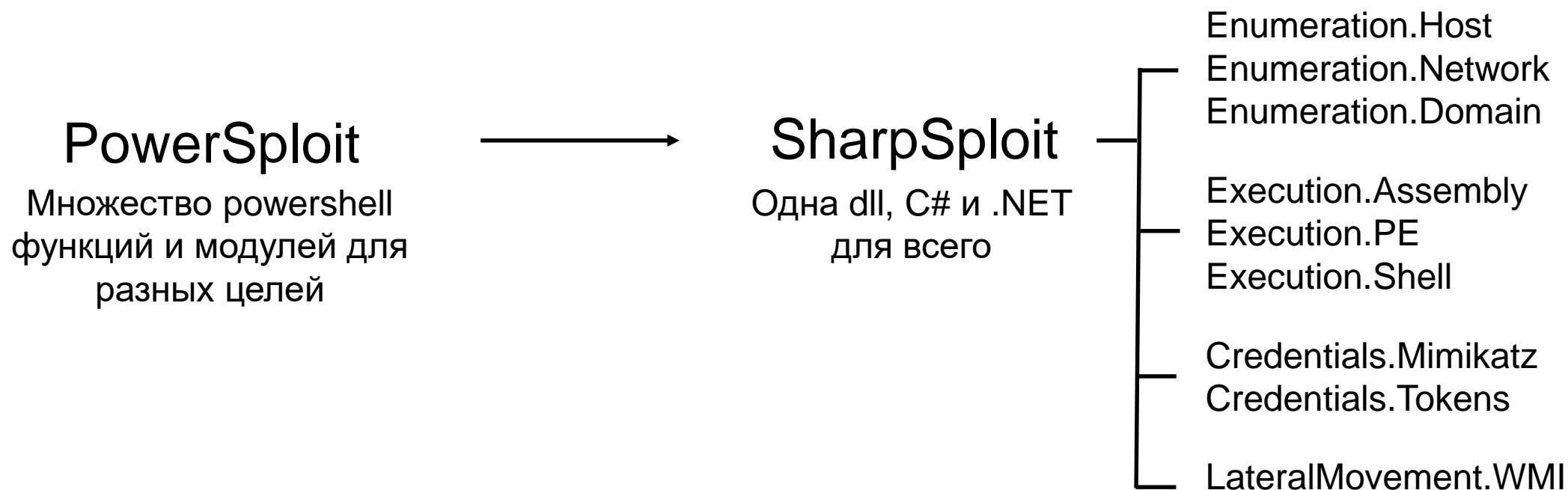
Действия злоумышленника

3. Дамп учетных данных на машине администратора AD



Действия злоумышленника

3. Дамп учетных данных на машине администратора AD

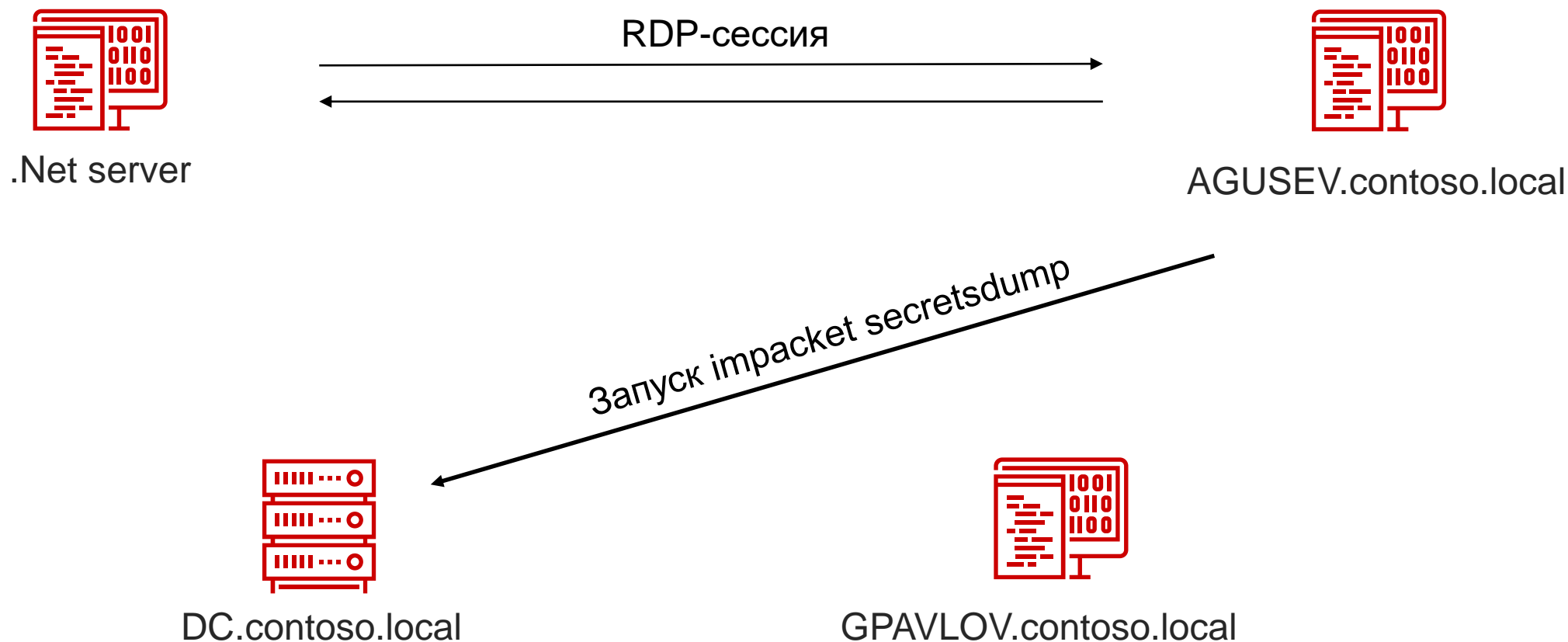


sharpsploit.cobbr.io/api/index.html

cobbr.io/SharpSploit.html

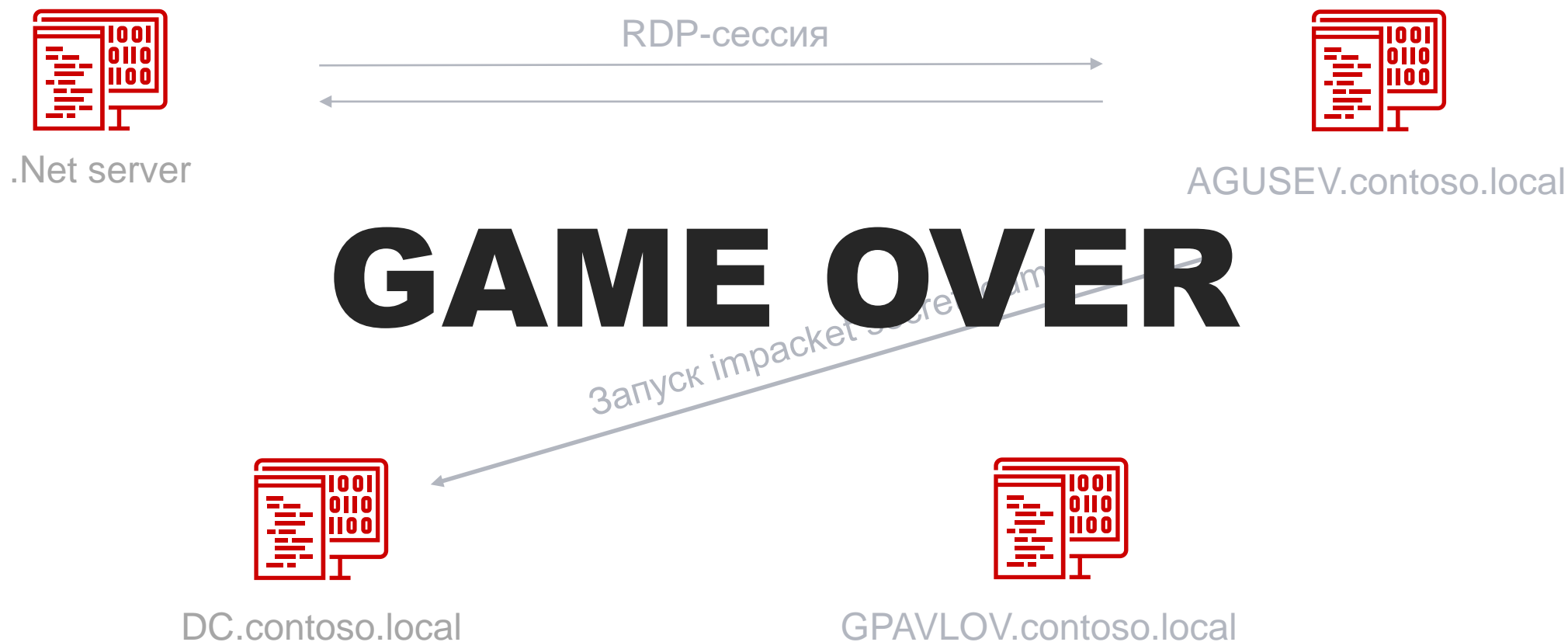
Действия злоумышленника

4. Получение дампа реестра DC с помощью secretdump



Действия злоумышленника

РТ



Действия злоумышленника



ATT&CK

Execution	Credential Access	Discovery	Lateral Movement
Service Execution	Credential Dumping	Remote System Discovery	Distributed COM
Powershell	Brute Force	Permission Groups Discovery	Windows Admin Shares
		Account Discovery	Remote Desktop Protocol
		Domain Trust Discovery	Remote File Copy

Обход защиты

- Выполнение через Distributed COM объекта Microsoft Management Console (MMC 2.0)
- Разрешенный протокол RDP
- Использование .NET-framework и assembly (SharpSploit)

PT

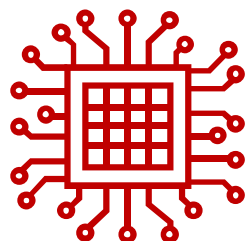
Как обнаружить латмув

ptsecurity.com



PT Network Attack Discovery — это ...

PT



PT NAD

Система глубокого анализа
сетевого трафика (NTA)
для выявления атак
на периметре и внутри сети.

NTA — решения класса Network Traffic Analysis

- **Мониторинг сети**
Видит все, что происходит
в трафике в режиме
реального времени
- **Выявление атак**
Пополнение правил
и индикаторов компрометации
2 раза в неделю
- **Расследования атак**
Хранит сырой трафик
и 1200 параметров сессий

PT

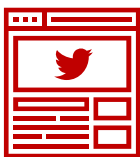
Как предотвратить подобные атаки



- Ограничить избыточное использование системных COM-объектов, не связанных с приложением (например, MMC 2.0)
- Блокировать учетные записи после большого количества ошибок аутентификации
- Ограничить права учетных записей helpdesk и использовать Just Enough Administration (JEA)
- Запретить удаленный вход для учетных записей локальных администраторов
- Блокировать использование System.Management.Automation.dll
(docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules)

Полезные ссылки

PT



Twitter

twitter.com/AttackDetection



Blog

habr.com/company/pt/blog/



**Threat Intelligence
отчеты и публикации**

ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/



**Проверить сеть
компании бесплатно:**

ptsecurity.com/ru-ru/products/network-attack-discovery/

Егор Подмоков

Специалист отдела экспертных сервисов PT ESC

t.me/PTNADChat