Тренды кибератак 2023. Как атакуют инфраструктуры компаний

SOC
FORUM
2023

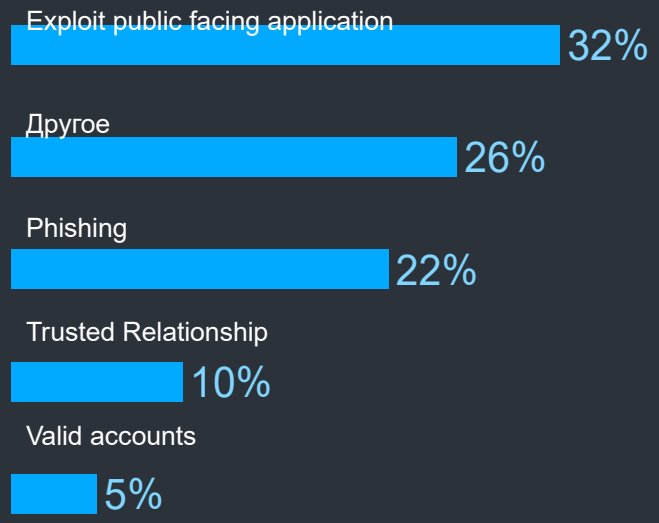
ИВАН СЮХИН

Руководитель группы расследования инцидентов
центра исследования киберугроз
Solar 4RAYS ГК «Солар»

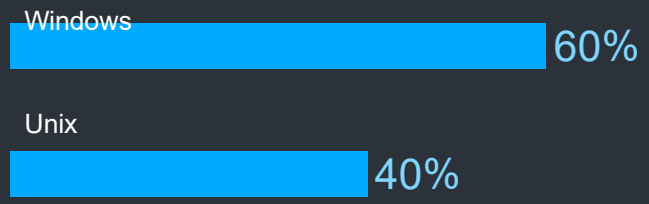
Статистика расследований в 2023 году

SOC FORUM 2023

ПЕРВОНАЧАЛЬНЫЙ ДОСТУП



ОПЕРАЦИОННЫЕ СИСТЕМЫ



I–III КВАРТАЛЫ 2023 Г.

21 КЕЙС

420 ИССЛЕДУЕМЫЕ СИСТЕМЫ

ТАЙМЛАЙН НАЧАЛА РАССЛЕДОВАНИЙ

Статистика расследований в 2023 году

SOC FORUM 2023

ДЛИТЕЛЬНОСТЬ АТАК В 2022

ДЛИТЕЛЬНОСТЬ АТАК В 2023

APT: тактики и техники

SOC FORUM 2023

INITIAL ACCESS	Exploit Public-Facing Application (ID: T1190), Phishing (ID: T1566)
PERSISTENCE	Windows Service (T1543.003) Scheduled Task/Job: Scheduled Task (ID: T1053.005), Web Shell (T1505.003) Valid Accounts: Domain Accounts (T1078.002)
DEFENCE EVASION	Hijack Execution Flow: DLL Side-Loading (T1574.002) Deobfuscate/Decode Files or Information (T1140), Indicator Removal (T1070) Masquerading: Masquerade Task or Service (T1036.004)
LATERAL MOVEMENT	Remote Services: Windows Remote Management (T1021.006) Remote Services: SSH (T1021.004) Remote Services: Remote Desktop Protocol (T1021.001) Remote Services: SMB/Windows Admin Shares (T1021.002)
CREDENTIAL ACCESS	OS Credential Dumping: NTDS (T1003.003), Security Account Manager (T1003.002), LSASS Memory (T1003.001) Brute Force: Password Spraying (T1110.003) Input Capture: Keylogging (T1417.001)
EXECUTION	Command and Scripting Interpreter: Windows Command Shell (T1059.003), PowerShell (T1059.001), Visual Basic (T1059.005), Python (T1059.006)

APT: тактики и техники, стоящие упоминания

Input = <ready_4-2024>

DEFENCE EVASION	Hide Artifacts: NTFS File Attributes (T1564.004) использование ADS Hide Artifacts: Process Argument Spoofing (T1564.010) подмена аргументов запуска Masquerading: Masquerade File Type (T1036.008) .png – не картинка! Masquerading: Break Process Trees (T1036.009) скрытие родителя Rootkit (T1014) rise of rootkit
PERSISTENCE	Server Software Component: IIS Components (T1505.004) модификация applicationHost.config Hijack Execution Flow (T1574) подмена легитимных файлов ОС Hijack Execution Flow: Dynamic Linker Hijacking (T1574.006) ld.so.preload Event Triggered Execution: Unix Shell Configuration Modification (T1546.004) \etc\sysconfig\network-scripts\ifup
CREDENTIAL ACCESS	Modify Authentication Process (T1556) модификация веток: HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\HwOrder

APT: тактики и техники, стоящие упоминания

SOC FORUM 2023

MALWARE

Custom malware:

Shadowpad, Shadowpad Light,

Ghost, TrochilusRAT, DonnectRAT,

DimanoRAT, PlugX

WEB SHELLS

Кастомные и публичные (Godzilla), China Chopper

CREDENTIAL ACCESS

CMPSpy, Inveigh, Mimikatz, goddi, secretsdump

REVERSE SHELL, PROXY

MicroSocks, SOCKS5, python-pty-shells

DISCOVERY

AdFind.exe, Sharphound

SCANNERS

Advanced IP Scanner, fscan, nbtscan, nmap

ROOTKIT

modified Azazel

CUSTOM SCRIPTS

ps1, vbs, python

LATERAL

WMIHACKER, Impacket

PRIVILEGE Escalation

PwnKit

Хактивизм Windows: тактики и техники

SOC FORUM 2023

INITIAL ACCESS	Exploit Public-Facing Application (ID: T1190), Phishing (ID: T1566)
PERSISTENCE	Registry Run Keys / Startup Folder (T1547.001), Windows Service (T1543.003), Scheduled Task/Job: Scheduled Task (ID: T1053.005), Web Shell (T1505.003) Valid Accounts: Domain Accounts (T1078.002) Create Account: Local Account T1136.001
DEFENCE EVASION	Deobfuscate/Decode Files or Information (T1140), Indicator Removal (T1070) Masquerading: Masquerade Task or Service (T1036.004)
LATERAL MOVEMENT	Remote Services: Windows Remote Management (T1021.006), Remote Desktop Protocol (T1021.001), SMB/Windows Admin Shares (T1021.002)
CREDENTIAL ACCESS	OS Credential Dumping: NTDS (T1003.003), Security Account Manager (T1003.002) Brute Force: Password Spraying (T1110.003), Input Capture: Keylogging (T1417.001)
EXECUTION	Command and Scripting Interpreter: Windows Command Shell (T1059.003), PowerShell (T1059.001), Visual Basic T1059.005
IMPACT	Data Destruction (T1485), Data Encrypted for Impact (T1486), Resource Hijacking (T1496)

Хактивизм Windows: тактики и техники, стоящие упоминания

SOC FORUM 2023

Exfiltration	Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
COMMAND AND CONTROL	Proxy (T1090) Qemu as tunnel: qemu-system-i386.exe -m 1M -netdev user,id=lan,restrict=off -netdev socket,id=sock,connect=92.XX.XX.214:444….
PERSISTENCE	Scheduled Task/Job: Scheduled Task «Невидимые задачи» Taskcache Boot or Logon Initialization Scripts: Logon Script (T1037.001) HKCU\Environment "UserInitMprLogonScript"
DEFENSE EVASION	Indirect Command Execution (T1202) WSL

SOCIAL ENGINEERING ON RISE

Хактивизм Windows: инструменты

SOC FORUM 2023

MALWARE

Public (Sliver, Cobalt Strike, meterpreter, PupyRAT, SystemBC, DarkGate, MeshAgent)

CUSTOM SCRIPTS

python, bat, vbs, ps1

WIPERs

custom, sdelete, Caddywiper

OTHER

RDP wrapper, Commando VM, Nhotkey

PROXY

socks2, socks

WEB SHELL

NeoReGeorg, tennc, Rebeyond Behinder (Ice Scorpion)

SCANNERS

Advanced Port Scanner, SoftPerfect Network Scanner, nmap

INITIAL ACCESS

public POC

CREDENTIALS ACCESS

mimikatz, cachedump64, procdump64, ntdsutil, secretsdump

LATERAL

Psexec, smbexec

Хактивизм Unix: тактики и техники

SOC FORUM 2023

INITIAL ACCESS	Exploit Public-Facing Application (ID: T1190), Valid Accounts (T1078)
PERSISTENCE	Create or Modify System Process: Systemd Service (T1543.002), Scheduled Task/Job: Cron (T1053.003), T1098.004 SSH Authorized Keys, **Hijack Execution Flow (T1574)**, Web Shell (T1505.003), Valid Accounts: Domain Accounts (T1078.002), Create Account: Local Account T1136.001
DEFENCE EVASION	Deobfuscate/Decode Files or Information (T1140), Indicator Removal (T1070), Masquerading: Masquerade Task or Service (T1036.004)
LATERAL MOVEMENT	Remote Services: SSH (T1021.004)
CREDENTIAL ACCESS	Input Capture: Keylogging (T1417.001)
EXECUTION	Command and Scripting Interpreter: Unix Shell (T1059.004)
IMPACT	Data Destruction (T1485), Data Encrypted for Impact (T1486), Resource Hijacking (T1496), Runtime Data Manipulation (T1565.003)

Хактивизм Unix: тактики и техники, стоящие упоминания

SOC FORUM 2023

PERSISTENCE
HIJACK EXECUTION FLOW (T1574)

Подмена PS\CD - User Execution PS\CD -> Wipe
Подмена pam_allow.so -> block access

PAM_ALLOW.SO – ПОДМЕНЕННАЯ ПРОГРАММА ДЛЯ ПЕРЕХВАТА ВЫЗОВА PAM_SM_AUTHENTICATE, ЧТО НЕ ПОЗВОЛЯЕТ ВОЙТИ В СИСТЕМУ

ВХОД ТОЛЬКО ПО 1 МАСТЕР-ПАРОЛЮ

Хактивизм Unix: инструменты

SOC FORUM 2023

MALWARE

Public (Sliver, PupyRAT, Meterpreter)

CUSTOM SCRIPTS

python, sh

WIPERs

custom, go-wiper

OTHER

freedesktop, Neofetch

PROXY

python-proxy, microsocks, chisel, ngrok

WEB SHELL

Godzilla, Rebeyond Behinder (Ice Scorpion), custom plugins

SCANNERS

nmap

INITIAL ACCESS

public POC

CREDENTIALS ACCESS

3snake, sshSPY, swap_digger, MimiPenguin, secretsdump

PRIVILEGE ESCALATION

PwnKit

ROOTKIT

modified Azazel

Итоги, тренды 2023

SOC FORUM 2023

ИДЕТ НА СПАД

- Количество атак майнеров

ОСТАЕТСЯ СТАБИЛЬНЫМ

- Высокая активность APT-групп
- Высокий поток фишинга

ИДЕТ НА УВЕЛИЧЕНИЕ

- Количество зараженных Unix-систем
- Уровень сложности атак хактивизма
- Частота использования rootkit
- Частота использования Social Engineering

АНОМАЛИИ

Все еще находим жертв proxylogon, proxyshell

Больше
практических кейсов,
результатов расследований
инцидентов от Solar 4RAYS

Input = <ready_4-2024>

i.syukhin@rt-solar.ru
ГК «Солар»
г. Москва