AZƏRBAYCANI HƏDƏF ALMIŞ KİBER TƏHDİD QRUPLARI HAQQINDA HESABAT

Kiber təhdid qrupları, hücum edilən ölkələr, hədəf alınan sahələr, istifadə olunan zərərli proqramlar, CVE-lər və hücum metodologiyaları barədə məlumatlar

Elektron Təhlükəsizlik Xidməti

Elektron
Təhlükəsizlik
Xidməti

ELEKTRON TƏHLÜKƏSİZLİK XİDMƏTİ HAQQINDA

Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidməti Azərbaycan Respublikası Prezidentinin 2012-ci il 26 sentyabr tarixli 708 nömrəli Fərmanının 5-ci hissəsinə əsasən yaradılıb.

Elektron Təhlükəsizlik Xidməti kibertəhlükəsizlik sahəsində informasiya infrastrukturu subyektlərinin fəaliyyətinin koordinasiyasını, mövcud və yarana biləcək elektron təhlükələr barədə ölkə səviyyəsində məlumatlandırmanı, əhalinin, özəl və digər qurumların kibertəhlükəsizlik sahəsində maarifləndirilməsini və onlara metodiki kömək göstərilməsini təmin edən icra hakimiyyəti orqanıdır.

Həmçinin Elektron Təhlükəsizlik Xidməti fəaliyyət istiqamətinə uyğun olaraq informasiya sistemlərinin və şəbəkələrinin, kompüter avadanlıqlarının və onların proqram təminatının, lokal və korporativ informasiya sistemlərinin və ehtiyatlarının təhlükəsizliyinə qarşı yönəldilmiş kiberhücumlar barədə məlumatları xarici ölkələrdəki analoji strukturlardan və digər mənbələrdən toplayır və təhlil edir.

ÜMUMİ MƏLUMAT

Elektron Təhlükəsizlik Xidməti tərəfindən aparılan araşdırmalar nəticəsində Azərbaycanın internet informasiya ehtiyatlarına hücumlar həyata keçirmiş kiber təhdid qrupları barədə hesabat tərtib olunub. Hesabatda təhdid qruplarının hücum etdiyi ölkələr, hədəf aldıqları sahələr, istifadə olunan zərərli proqramlar, CVE-lər, hücum metodologiyası barədə məlumatlar yer alıb. Hesabat tərtib olunarkən APT qrupların araşdırılmasında bəzi məlumatların əldə olunması üçün "MITRE ATT&CK" platformasına istinad edilib.

APT (Qabaqcıl Davamlı Təhdid)

Əsasən dövlətlər, müəssisələr kimi konkret hədəfləri olan davamlı olaraq sistemlərə sızma proseslərində iştirak edən kiber təhdid qruplarıdır. Adətən dövlətlər tərəfindən maliyyələşdirilən bu qruplar casusluq, məlumat oğurluğu və ya təxribatlarla məşğul olurlar. Onlar məqsədlərinə çatmaqda əzmkarlıqları, yüksək bacarıq səviyyəsi və əhəmiyyətli resursları ilə xarakterizə olunur ki, bu da onlara sızmaq və uzun müddət aşkar edilmədən kompüter sistemləri daxilində qalmaq üçün geniş çeşidli üsullardan istifadə etməyə imkan verir. APT qrupları sistemdə aşkarlanmamaq üçün qabaqcıl zərərli proqramlardan istifadə edərək kiberhücumlar həyata keçirməsi tanınırlar.

MITRE | ATT&CK®

MITRE ATT&CK (Adversarial Tacticks, Techniques and Common Knowledge) - Kiber monitorinq araşdırmalarına əsaslanaraq təhdid qruplarının taktika və texnikalarına qlobal olaraq əlçatanlığı təmin edən platformadır. Burada qeyd olunan məlumatlar özəl sektorda, dövlətdə və kibertəhlükəsizlik icmalarında xüsusi təhdid modelləri və metodologiyaların inkişafı üçün istifadə olunur.
Platformaya əsəsən, təhdid qruplarının hücum metodologiyası bir neçə istiqamətdə sinifləndirilib. Bura daxildir:

Hədəf sistemə ilkin giriş

Qrup hədəf sistemə giriş əldə etmək üçün fişinq e-poçtları, proqram istismarı və ya sosial mühəndislik də daxil olmaqla müxtəlif üsullardan istifadə edir.

Sistemdə davamlı qalmaq

İlkin giriş əldə edildikdən sonra qrup sistemdə möhkəmlənməyə çalışır. Bu, adətən sistem üzərində daimi giriş və nəzarət əldə etməsinə imkan verən zərərli kodun yüklənməsini və icrasını əhatə edir.

Sistemdə aşkarlanmamaq

Qrupun ələ keçirilmiş sistemdə aşkarlanmadan qalmağa çalışdığı mərhələdir. Belə ki, qabaqcıl yayınma üsullarından istifadə edərək və təhlükəsizlik tədbirlərinə uyğunlaşaraq, uzun müddət ərzində öz zərərli fəaliyyətlərini həyata keçirməyə imkan verən davamlılığını qorumağa çalışırlar.

İmtiyazların artırılması

Qrup daha sonra sistem daxilində daha yüksək səviyyəli giriş əldə etmək üçün imtiyazları artırmağa çalışır. Bu proses sistemin yanlış konfiqurasiya olunması, zəif şifrlərin istifadəsi və ya daxili sistemlərdəki boşluqlar nəticəsində baş verir.

İnfrastrukturdaxili kəşfiyyat

Qrup əldə etdiyi imtiyazlarla hədəf şəbəkə haqqında məlumat toplamaq və həssas məlumatları müəyyən etmək üçün infrastrukturdaxili kəşfiyyat həyata keçirir. Kəşfiyyat zamanı məxfi faylların axtarışı, hədəf alınacaq digər sistemlərin müəyyən edilməsi və ya şəbəkə topologiyasının xəritələşdirilməsi həyata keçirilir.

Şəbəkədaxili hərəkət

Qrup ələ keçirdiyi cihazlar vasitəsi ilə digər sistemlərə daxil olmaq üçün şəbəkə daxilində hərəkət edir. Bu, onlara daha çox sistemə nəzarət etməyə və kritik serverlər kimi yüksək əhəmiyyətli hədəfləri ələ keçirməyə imkan verir.

Hücumun tamamlanması

Hücumun nəticəsinə uyğun olaraq məlumatların oğurlanması, əməliyyatların dayandırılması, fidyə proqramlarının yayılması və ya gələcək girişlər üçün backdoor-ların quraşdırılması kimi hadisələr baş verir.

İstifadə olunan terminlərin izahı

Keylogger - İstifadəçinin klaviatura əməliyyatlarını gizli şəkildə qeyd edən, çox vaxt şifrlər və bank kartı kimi həssas məlumatları ələ keçirmək üçün istifadə edilən proqram və ya cihazdır.

Spear-phishing - Konkret şəxsin həssas məlumatlarını oğurlamaq üçün saxta e-poçt, mətn və telefon zənglərindən istifadə edilərək həyata keçirilən kiber hücumdur.

Log4j2 –"Java" əsaslı qeyd (log) üçün nəzərdə tutulmuş yardımçı proqramdır.

Ransomware - İstifadəçi fayllarının şifrələnməsində və daha sonra onların geri qaytarılmasında istifadə olunan ödəniş tələb edən zərərli proqramdır.

Web shell – Veb-serverlərə daxil olmağa və orada qalıcılığı saxlamağa imkan verən zərərli skriptlərdir.

Active directory – "Windows" mühitində şəbəkə resurslarını təşkil və idarə edən, mərkəzləşdirilmiş autentifikasiya, avtorizasiya və kataloq xidmətlərinə imkan verən "Microsoft" xidmətidir.

"Supply chain attack"- Sadə dildə desək, "Təchizat zənciri hücumu"dur. Bu hücum növündə əsas məqsəd, müəssisələrə 3-cü tərəf şirkətlər vasitəsilə proqram və ya texniki təminatına ciddi zərər vurmaqdır.

ASEP –"Windows"da proqram tərtibatçılarına sistemin yüklənməsi və ya istifadəçinin daxil olması zamanı proqramları avtomatik işə salmağa imkan verir.

Mimikatz – "Windows" əməliyyat sistemlərinin yaddaşından şifrlər kimi həssas məlumatları çıxarmağa, icazəsiz girişə və s. bir çox fəaliyyətə imkan verən zərərli proqramdır.

Windows Management Instrumentation (WMI) - Windows əsaslı əməliyyat sistemlərində sistem və cihaz idarəetmə tapşırıqları üçün çərçivə (framework) təmin edən "Microsoft" texnologiyasıdır.

Domen nəzarətçisi - İstifadəçilərin autentifikasiyası, resurslara girişin verilməsi və domen daxilində təhlükəsizlik siyasətlərinin tətbiqi üçün cavabdeh olan serverdir.

Modul - Bir və ya daha çox funksiyaları ehtiva edən proqramın bir hissəsidir.

Macro - Təkrarlanan tapşırıqları avtomatlaşdırmaq üçün istifadə edilən hərəkətlərin və ya əmrlərin ardıcıllığıdır.

.CHM faylı – Mətn, şəkillər, hiperlinklər və digər məzmunlu sıxılmış HTML faylıdır.

ZIP, RAR faylları- Faylın yaddaş ölçüsünü səmərəli şəkildə azaldan və paylanmağı asanlaşdıran fayl sıxılma formatlarıdır.

HTML faylı – Veb-səhifənin strukturunu və məzmununu ehtiva edən fayldır.

RDP – İstifadəçiyə şəbəkə üzərindən kompüterə qoşulmağa və idarə etməyə imkan verən protokoldur.

.NET - "Microsoft" tərəfindən hazırlanmış bir çox proqramlaşdırma dillərini və kitabxanaları dəstəkləyən proqram təminatı çərçivəsidir (framework)

PowerShell – "Windows" mühitlərində təkrarlanan tapşırıqların avtomatlaşdırılmasını sadələşdirmək üçün nəzərdə tutulmuş skript dilidir.

TOR – məxfiliyi və təhlükəsizliyi artırmaq məqsədi daşıyan anonim şəbəkədir.

Cobalt Strike – Gizli ünsiyyət və imtiyazların artırılması kimi məqsədlər üçün istifadə olunan proqramdır.

.BAT faylı – Ardıcıllıqla bir sıra əmr və ya təlimatları avtomatlaşdırmaq üçün istifadə olunan fayldır.

Windows CertUtil – Müxtəlif sertifikat əməliyyatları, o cümlədən faylların kodlaşdırılması və deşifrə edilməsi, sertifikat məlumatlarının göstərilməsi və sertifikat xidmətlərinin idarə edilməsi üçün istifadə olunan köməkçi proqramdır.

Dropbox – İstifadəçilərə faylları onlayn saxlamağa və paylaşmağa imkan verən xidmətdir.

.MSI file – Faylların quraşdırma prosesi üçün lazım olan quraşdırma məlumatlarını, faylları və konfiqurasiyanı ehtiva edən proqram təminatının quraşdırılması üçün istifadə olunan fayl formatıdır.

XML – Həm insan tərəfindən oxuna bilən, həm də maşın tərəfindən oxuna bilən, məlumatların iyerarxik formatda strukturlaşdırılması və saxlanması üçün geniş istifadə olunan çox yönlü işarələmə (markup) dilidir.

İstifadə olunan terminlərin izahı

RDP (Remote Desktop Protocol) - Microsoft tərəfindən hazırlanmış xüsusi protokoldur, istifadəçilərə uzaqdan kompüterə şəbəkə üzərində qoşulmağa və idarə etməyə imkan verir, uzaqdan giriş və idarəetmə üçün qrafik istifadəçi interfeysi ilə təmin edir.

VPN (Virtual Private Network)- İnternet üzərindən təhlükəsiz və şifrəli əlaqə yaradan, istifadəçilərə uzaq məsafədən şəxsi şəbəkəyə daxil olmağa imkan verən və ötürülən məlumatların məxfiliyini təmin edən texnologiyadır.

Rust – Təhlükəsizlik və performans üstünlüyü kimi bir çox funksiyaya malik proqramlaşdırma dilidir.

VBA – "Microsoft" tərəfindən hazırlanmış proqramlaşdırma dilidir və istifadəçilərə "Microsoft Office" proqramlarında tapşırıqları avtomatlaşdırmağa, makrolar yaratmağa və funksiyaları fərdiləşdirməyə imkan verir.

VBScript dropper – Zərərli proqramların quraşdırılmasına başlamaq və ya hədəf sistemdə digər zərərli fəaliyyətlər üçün istifadə olunur.

Affine – Açıq mətni şifrəli mətnə çevirmək üçün riyazi əməliyyatlardan istifadə edən kriptoqrafik texnikadır.

Windows Credential Manager – Proqramlar və veb-saytlar üçün istifadəçi adlarını və şifrləri təhlükəsiz şəkildə saxlayan və idarə edən, istifadəçinin autentifikasiyasını asanlaşdıran "Windows" funksiyasıdır.

Şablon faylı (.dotm) – Əvvəlcədən müəyyən edilmiş stilləri, formatları, makroları və digər elementləri ehtiva edən və strukturu olan sənədlərin yaradılması üçün "Microsoft Word" sənəd şablonudur.

RTF – Müxtəlif mətn prosessorları və əməliyyat sistemləri arasında formatlaşdırılmış mətn və qrafiklərin mübadiləsinə imkan verən, əsas sənəd strukturunu və formatlaşdırmanı qorumaq üçün ümumi formatı təmin edən fayl formatıdır.

Sənaye idarəetmə sistemləri (ICS) - İstehsal və ya kritik infrastrukturda müxtəlif əməliyyatları idarə etmək və avtomatlaşdırmaq üçün aparat, proqram təminatı və şəbəkə komponentlərindən ibarət olan kompüter əsaslı sistemdir.

Domen üzvlüyü - Mərkəzləşdirilmiş idarəetməni və girişə nəzarəti asanlaşdıran, "Windows" domen şəbəkəsi ilə əlaqəli kompüter və ya istifadəçi hesabının statusudur.

Drayver - Kompüter sisteminin aparat və proqram təminatı arasında qarşılıqlı əlaqəni asanlaşdıran vasitəçi proqramlardır.

.Lnk faylı – "Microsoft Windows"da başqa fayl və ya proqrama istinad və ya keçid kimi istifadə edilən fayl növüdür.

.Hta faylı – "Windows"da qrafik interfeysləri olan proqramlar yaratmaq üçün HTML, CSS və JavaScript istifadə edən, icra edilə bilən fayl növüdür.

Vhdx – "Microsoft Hyper-V" tərəfindən virtual maşının məzmununu saxlamaq üçün istifadə edilən virtual sabit disk faylıdır.

Backdoor - Kompüter sisteminə, proqram təminatına və ya şəbəkəyə daxil olmaq üçün autentifikasiya və ya şifrələmədən yan keçməyə imkan verən metoddur.

CVE - İctimaiyyətə məlum olan kibertəhlükəsizlik zəifliklərı üçün unikal identifikatorlar (CVE ID-ləri) təmin edən və təhlükəsizlik icmaları arasında məlumatların paylaşılmasını asanlaşdıran sistemdir.

Remote access trojan - Uzaqdan hücum üçün hədəfin kompüterinə və ya şəbəkəsinə icazəsiz giriş və nəzarət əldə etməyə imkan verən zərərli proqramdır.

Plagin - Kompüter proqramlarına, tətbiqlərə və veb-saytlara yeni xüsusiyyətlər əlavə edərək fərdiləşdirilməsinə imkan verən proqram əlavəsidir.

Patch - Kompüter proqramında, əməliyyat sistemində və ya tətbiqdə boşluqları aradan qaldırmaq və ya təhlükəsizlik problemlərini həll etmək üçün nəzərdə tutulmuş kod və ya proqram yeniləməsidir.

Router - Məlumatların səmərəli və təhlükəsiz şəkildə ötürülməsinə imkan verən, yerli şəbəkədəki cihazlar və internet arasında internet trafikini yönləndirən cihazdır.

Switch - Lokal şəbəkədə kompüterlər, printerlər və serverlər daxil olmaqla bütün cihazları birləşdirərək resursların paylaşılmasını asanlaşdırır.

Mündəricat

Azərbaycanı hədəf almış

Kiber təhdid qrupları

- MuddyWater
- Electrum
- Leviathan
- Red October
- Slience
- Inception Framework
- Cozy Bear
- Turla
- Fancy Bear
- Gananite
- Stibnite
- Soleimani Cyber Army
- YoroTrooper
- OilRig
- EbRaHIM-VaKeR

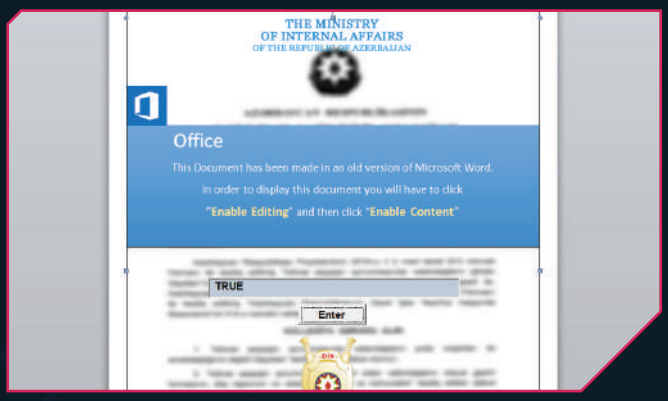
MuddyWater

2017-ci ildən fəaliyyət göstərən "MuddyWater" İranın Kəşfiyyat və Təhlükəsizlik Nazirliyinin (MOIS) tabeliyində olduğu ehtimal edilən kiber təhdid qrupudur. "Earth Vetala", "MERCURY", "Static Kitten", "Seedworm", "TEMP.Zagros" adları ilə tanınan qrupun əsas hücum hədəfləri dövlət orqanları, telekommunikasiya və neft şirkətləridir. Qrupun hədəf aldığı ölkələr sırasına İordaniya, Türkiyə, Azərbaycan, Pakistan, Əfqanıstan, İraq və Səudiyyə Ərəbistanı daxildir.
"MuddyWater"in qeydə alınan ən son hücumlarından biri 2022-ci ilin yanvar ayında Türkiyədəki dövlət qurumlarına və özəl şirkətlərə olmuşdur. Hücum zamanı qrup, Türkiyənin Səhiyyə və Daxili İşlər Nazirliyinin adından istifadə edərək, istifadəçiləri aldatmağa çalışmışdır.

Qrupa aid CVE-lər:

CVE-2022-45359, CVE-2022-47633, CVE-2017-0199, CVE-2021-45608, CVE-2017-0213, CVE-2020-1472, CVE-2021-44228, CVE-2018-20250, CVE-2021-45046, CVE-2020-0688, CVE-2018-13379

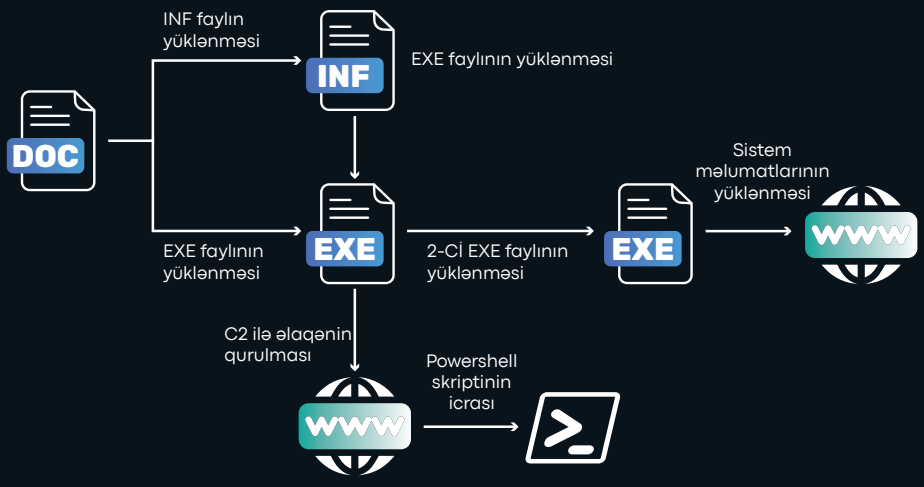
Şəkil 1-də "MuddyWater" qrupunun Azərbaycana qarşı "spear fişinq" hücumlarını həyata keçirərkən istifadə etdiyi nümunəni görə bilərik. Bu hücum cəhdində əsas məqsəd, istifadəçiləri macro-ları aktivləşdirməyə yönəltməkdir. Qrup bu növ hücumlarını həyata keçirmək üçün istifadəçilərin etibarlı hesab etdiyi ələ keçirilmiş cihazlardan istifadə etmişdir.



Şəkil 1. Zərərli "MS Office" sənədi

Qrupun hücum metodologiyası

Qrup hücumlarını adətən zərərli kodlarla təchiz olunmuş "Microsoft Office" fayllarını e-poçt ilə hədəfə göndərərək və ya proqram təminatında aşkarlanan boşluqlar vasitəsilə həyata keçirir. Hədəf sistemə daxil olduqdan sonra orada davamlı qalmaq üçün müxtəlif vasitələrdən, o cümlədən uzaqdan giriş troyanlarından (remote access trojan) və backdoor-lardan istifadə edirlər.



Qrafik 1. Muddy Water yoluxma zənciri

Bununla yanaşı qrup hədəfin sisteminə zərərli proqram təminatını quraşdırmaq üçün "spear-phishing" və sosial mühəndislik metodlarından da istifadə edir. Belə ki, daxilində "macro" olan "Microsoft Office" sənədi hədəf sistemə yüklənilir. "Macro" aktivləşdikdə "INF" və "EXE" tipli zərərverici proqramlar sistemə yüklənir. "INF" faylı, sistemdə davamlılığı təmin etmək və istifadəçi sistemə daxil olduqda əsas zərərvericinin işə düşməsi üçün registr açarlarına dəyişiklik edir. Əsas zərərverici proqram (EXE faylı) isə öz növbəsində sistem və şəbəkə məlumatlarını toplayır və bu məlumatları göndərmək üçün 2-ci zərərvericini yaradır. Qrup tərəfindən göndərilən təlimatlar "Powershell" faylına yazılır və əsas zərverici tərəfindən icra edilir.

MuddyWater qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

PowGoop - "DLL" yükləyici və "PowerShell" əsaslı yükləyicidən ibarət olan zərərli proqram yükləyicisidir. Bu yükləyici, zərərli serverlərə "HTTP GET" sorğuları göndərə, "PowerShell" skriptləri vasitəsilə əmrləri icra edə və məlumatları şifrələmək üçün modifikasiya olunmuş "Base64" kodlamasından istifadə edə bilir. Həmçinin proqram "Goopdate.dll" fayllarını "GoogleUpdate.exe"yə köçürə bilir, həmçinin ".dot" (goopdate.dat) faylı adı altında maskalanır. "PowGoop" özünü "Google update"in rəsmi faylı olduğunu göstərmək üçün "Goopdate.dll"dən istifadə edir.

Small Sieve - "Telegram Bot API" əsaslı Python backdoor-udur və "Nullsoft Scriptable Install System" (NSIS) quraşdırıcısı vasitəsilə yayılmışdır. Proqram, xaker tərəfindən idarə olunan C2 serverləri ilə "Telegram API" üzərindən HTTPS vasitəsilə əlaqə saxlaya, "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift" yolu vasitəsi ilə sistemdə davamlılıq əldə edə, "cmd.exe" və "Python" skriptləri ilə sistemdə əmrləri icra edə bilər.

Mori - C2 ilə əlaqəsi qurmaq üçün "DNS tunelling" protokolundan və "Base64" ilə kodlanmış "JSON" kitabxanalarından istifadə edən backdoor-dur. Mori, "HKLM\Software\NFC\IPA" və "HKLM\Software\NFC" daxil olmaqla, registrdən məlumatları oxuyur və dəyişdirir, "DLL" icrası üçün "regsvr32.exe"dən istifadə edə bilir.

POWERSTATS - "PowerShell", "VBScript" (VBE) və "JavaScript" kodundan istifadə edərək təhlükəsizlik həllərindən yayına bilən "PowerShell" əsaslı backdoor-dur. C2 trafikini "base64" və "RSA" ilə şifrələyən proqram, "Microsoft Office Protected View" rejimini deaktiv edə və "PowerShell" əmrləri icra edə bilər. Bu proqram, "MicrosoftEdge" adlı planlaşdırılmış bir tapşırıq yaradaraq, sistemdə davamlılıq qura və məlumatları ələ keçirə bilər.

ELECTRUM

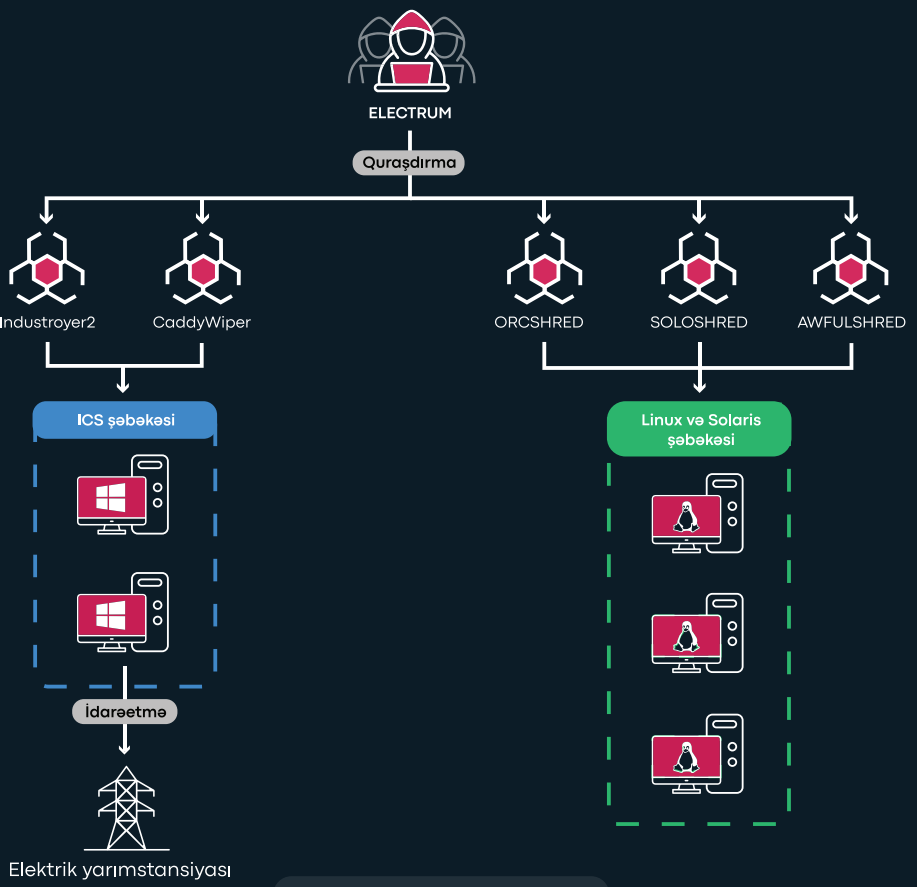
2017-ci ildən fəaliyyət göstərən qrupun müxtəlif mənbələrdə İran İslam respublikası ilə əlaqəli olduğu qeyd edilir. "Telebots", "IRON VIKING", "BlackEnergy", "Quedagh", "Voodoo Bear", "IRIDIUM" adları ilə tanınan qrupun əsas hücum hədəfləri başda kommunal xidmətlər sektoru olmaqla, səhiyyə, telekommunikasiya, media, istehsalat, bank və müdafiə sektorudur. Qrupun hədəf aldığı ölkələr sırasına Avstraliya, Azərbaycan, Belarusiya, Danimarka, Fransa, Gürcüstan, Hindistan, İran, İslam Respublikası, İsrail, Qazaxıstan, Koreya, Respublikası, Qırğızıstan, Litva, Polşa, Rusiya Federasiyası, Sinqapur, Ukrayna, Böyük Britaniya və ABŞ daxildir. Qeydə alınmış ən son hücumlarından biri 2022-ci ildə Ukraynanın elektrik yarımstansiyasına olmuşdur. Həyata keçirilən hücum dağıdıcı təsirləri ilə yadda qalmışdır.

Qrupa aid CVE-lər:

CVE-2021-44228, CVE-2014-4114, CVE-2013-3906, CVE-2022-39952

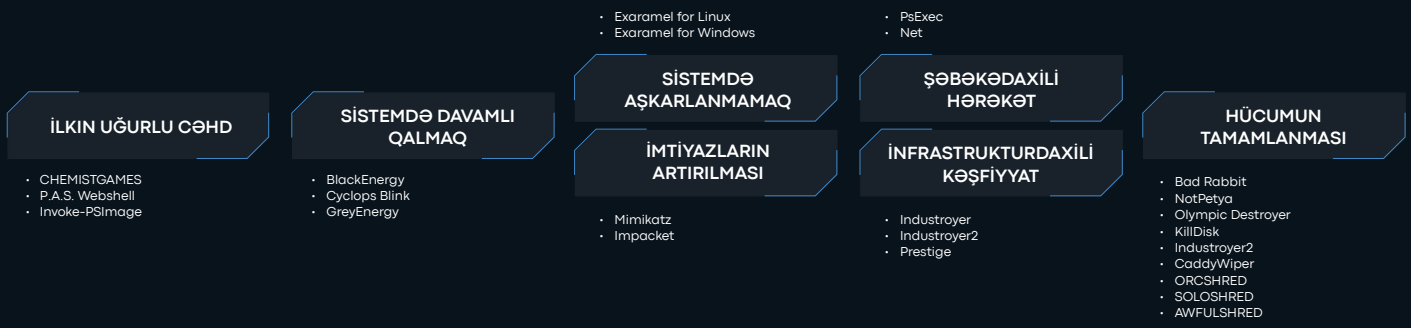
Qrupun hücum metodologiyası

ELECTRUM qrupu, həmçinin kriptovalyuta birjalarına və istifadəçilərinə yönəlmiş hücumlarda iştirak etməsi ilə tanınan qrupdur. Kiberhücumlarında əsasən, uzaqdan giriş troyanları və keylogger-lər də daxil olmaqla bir çox zərərli proqramlardan və yüksək səviyyədə hazırlanmış sosial mühəndislik metodundan istifadə edirlər. Qrupun daha çox Windows və MacOS əməliyyat sistemlərini hədəf aldığı müəyyən olunub.



Qrafik 2. Electrum yoluxma zənciri

Qrafik 2-də "ELECTRUM" qrupunun "Industroyer2", "CaddyWiper", "ORCSHRED", "SOLOSHRED" və "AWFULSHRED" kimi zərərli proqramları hansı hədəf sistemə yükləməsi təsvir olunub. Zərərli proqramlardan "Industroyer2" sənaye idarəetmə sistemlərinin (ICS) fəaliyyətinə zərər vurur, "CaddyWiper" isə hədəflənmiş cihazlardan məlumatları silir. "ORCSHRED", "SOLOSHRED" və "AWFULSHRED" enerji şirkətlərinin şəbəkəsində Linux və Solaris əməliyyat sistemləri üçün hazırlanmış zərərli proqramlardır və əsas funksiyaları şəbəkədaxili hərəkət etmək, sistemə bağlı olan yaddaş qurğularındakı məlumatları silməkdir.



Electrum qrupunun hücum zamanı istifadə etdiyi proqramlar

BlackEnergy – Paylanmış Xidmətdən imtina (DDoS) hücumlarında botnetlər yaratmaq üçün nəzərdə tutulmuşdur. Lakin daha sonra müxtəlif plaqinləri dəstəkləyən mürəkkəb zərərli proqrama çevrilmişdir. "BlackEnergy2" və "BlackEnergy3" kimi variantları da var.

Invoke - "PSImage PowerShell" skriptinin baytlarını "PNG" şəklinin piksellərinə yerləşdirir. Proqramın işləmə mexanizmi isə "Invoke-Mimikatz" modulundan istifadə edərək, "PowerShell" skriptini şəkil faylına yerləşdirməkdir. Belə ki, proqram macro-dan şəkil faylına əlaqə yaradaraq, "PowerShell" skriptini icra edir. Daha sonra skript macro kodundan istifadə edərək, şifrləri sızdıra bilir.

KillDisk - Əməliyyat sisteminin fəaliyyətini dayandırmağa kömək edən proqram, ilk dəfə 2015-ci ildə Ukraynaya qarşı kiberhücumlar zamanı "BlackEnergy" zərərli proqram təminatının tərkib hissəsi kimi istifadə olunub. 2016-cı ildə bəzi "KillDisk" variantlarına "ransomware" komponenti də daxil edilmişdir.

Net utility- "Windows" əməliyyat sisteminin tərkib hissəsidir. İstifadəçilərə, qruplara, xidmətlərə və şəbəkə bağlantılarına nəzarət etmək üçün əmr əməliyyatlarında istifadə olunur. Alət bir çox funksiyaya malikdir, bunlara misal olaraq kəşfiyyat üçün sistem və şəbəkə məlumatlarının toplanması, "net use" əmrlərindən istifadə edərək, "SMB/Windows" admin qovluqlarında şəbəkədaxili hərəkət və xidmətlərlə qarşılıqlı əlaqə kimi çoxsaylı imkanlar daxildir.

Leviathan

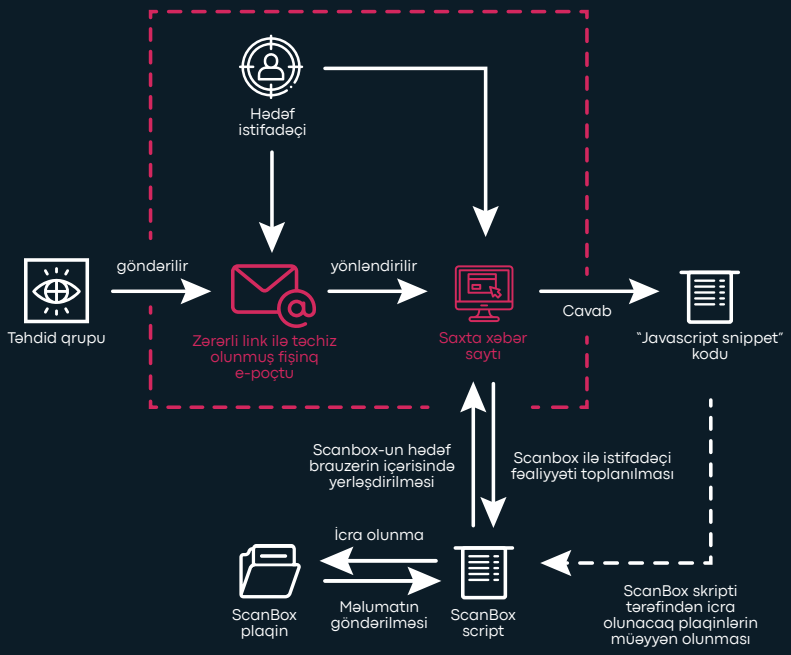
2014-cü ildən fəaliyyət göstərən kiber təhdid qrupunun Çində respublikasına məxsus olduğu təxmin edilir. "MUDCARP", "Kryptonite Panda", "Gadolinium", "BRONZE MOHAWK", "TEMP.Jumper", "APT40", "TEMP.Periscope" adları ilə tanınan qrupun əsas hücum hədəfləri başda dövlət orqanları olmaqla, gəmiçilik, nəqliyyat, istehsal şirkətləri və tədqiqat universitetləridir. Qrupun hədəf aldığı ölkələr sırasına Argentina, Ermənistan, Avstraliya, Avstriya, Azərbaycan, Belarus, Belçika, Braziliya, Bruney, Kamboca, Kanada, Çin, Kolumbiya, Kosta Rika, Fransa, Almaniya, Haiti, Macarıstan, Hindistan, İraq, İsrail, İtaliya, Yaponiya, Qazaxıstan, Qırğızıstan və s. daxildir.
Qrup tərəfindən həyata keçirilən fişinq hücumlarına 2017-ci ildə ABŞ-ın gəmiqayırma şirkətini və hərbi əlaqələri olan Universitet Tədqiqat Mərkəzini, 2018-ci ildə isə Böyük Britaniyada yerləşən mühəndislik şirkətini misal göstərmək olar.

Qrupa aid CVE-lər:

CVE-2022-30190, CVE-2022-26766, CVE-2022-2294, CVE-2018-8570, CVE-2019-6225, CVE-2017-11882, CVE-2018-0798, CVE-2014-1761, CVE-2012-0158, CVE-2015-7645, CVE-2016-1019, CVE-2018-0802, CVE-2017-8570, CVE-2016-4117, CVE-2017-0199

Qrupun hücum metodologiyası

"Leviathan" qrupu adətən bir qurumun informasiya ehtiyatlarına hücum etmək üçün üçüncü tərəf şirkətlərdən istifadə edir. Belə ki, üçüncü tərəf şirkətlərin domen adına oxşar və ya sistemləri ələ keçirilmiş şirkətin resurlarından istifadə edərək zərərverici proqramla təchiz olunmuş faylları, keçidləri e-poçt vasitəsi ilə hədəflərə göndərirlər. Əsasən "Orz" və "NanHaiShu" kimi tanınan zərərli proqramlardan istifadə edirlər.



Qrafik 3. Leviathan yoluxma zənciri

Qrafik 3-də təhdid qrupunun ilk olaraq hədəfə daxilində zərərli link olan e-poçt göndərilməsi təsvir olunub. İstifadəçi zərərli keçidə kliklədikdə keçid istifadəçini qrup tərəfindən idarə olunan serverdə yerləşdirilirmiş saxta xəbər saytına yönləndirir. Serverdə hədəf sistemin məlumatlarını skan etmək üçün nəzərdə tutulmuş və "Javascript" kodunun bir hissəsi olan "ScanBox" skripti mövcuddur. Qrup hədəf kompüterdə hansı plaqinləri icra olunacağını müəyyən etmək üçün bu məlumatlardan istifadə edir. Bu plaqinlər məlumatları oğurlamaq və növbəti zərərli fəaliyyətlər üçün nəzərdə tutulub.

Leviathan qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

China Chopper - "HTTP POST" əmrləri vasitəsilə kod icrasını, "brutforce" hücumlarını, fayl əməliyyatlarını və kataloq siyahısını dəstəkləyən veb serverlər vasitəsilə backdoor girişi üçün hazırlanmış web shell-dir. Çoxyönlü olması ilə tanınır və bir çox təhdid qrupları tərəfindən istifadə olunur.

gh0st RAT - Sistemdə davamlılıq, uzaqdan əmr icrası, C2 əlaqələri üçün məlumatların şifrələnməsi, event log-ların silinməsi və klaviatura qeydlərini əldə etmək üçün istifadə olunan uzaqdan giriş troyanıdır (RAT). C2 üçün dinamik DNS-dən istifadə edir və istifadəçinin ekran görüntüsünü və fayllarını yükləyə bilir.

PowerSploit - Token manipulyasiyası, imtiyazların artırılması, audio qeyd alma, sistemdə davamlılıq və antivirusdan yayınma üçün modullar təklif edən "PowerShell" moduludur. Alət, istifadəçi məlumatlarını toplamaq, skript modifikasiyası və kod icrasını həyata keçirir.

MURKYTOP - Əməliyyat sistemi məlumatlarının toplanması, fayl silinməsi, port skanlaması və tapşırıq planlaşdırılmasında istifadə olunan kəşfiyyat alətidir.

Red October

"The Rocra" kimidə tanınan qrup ilk dəfə 2012-ci ildə müəyyən olunub. Qrupun Rusiya federasiyası ilə əlaqəli olduğu ehtimal edilir. Əsas hücum hədəfləri tədqiqat universitetləri, aerokosmik sektorlara yanaşı, müxtəlif ölkələrin diplomatik nümayəndəlikləri və dövlət qurumlarıdır. Hədəf aldıqları ölkələr sırasına Rusiya Federasiyası, Qazaxıstan, Azərbaycan, Belçika, Hindistan, Əfqanıstan, Ermənistan, İran İslam Respublikası, Türkmənistan, Ukrayna, ABŞ, Vyetnam, Belarusiya, Yunanıstan, İtaliya, Mərakeş, Pakistan, İsveçrə, Uqanda, Birləşmiş Ərəb Əmirlikləri daxildir.

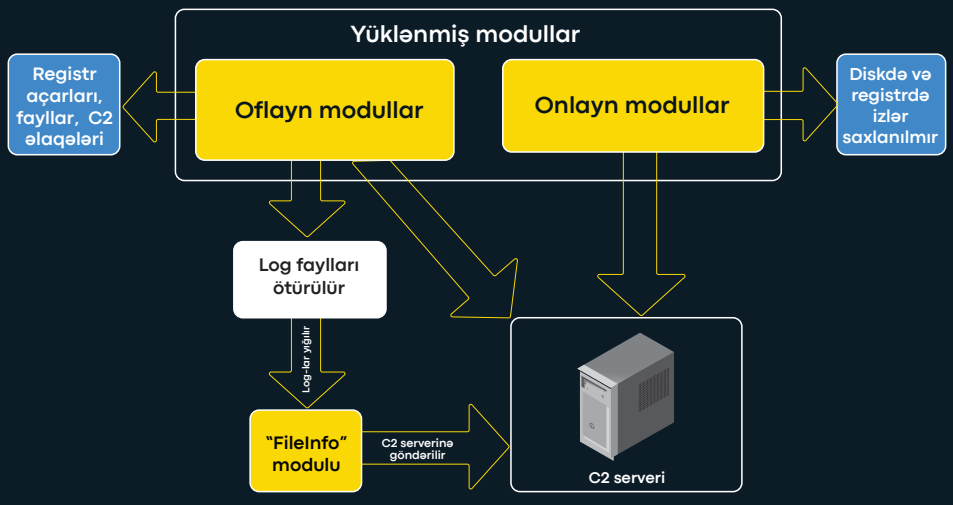
Qrupa aid CVE-lər:

CVE-2009-3120, CVE-2010-3333, CVE-2012-0158, CVE-2009-3129

Qrupun hücum metodologiyası

"Red October" qrupu hücumlarını daha kompleks şəkildə etmək üçün müxtəlif sistemlərin konfiqurasiyalarına tez uyğunlaşa bilən, bir neçə zərərli faylları özündə birləşdirən zərərli proqram hazırlamışdır. Bu yeni zərərli proqram bir neçə xüsusiyyətlərə malikdir. Bu xüsusiyyətlərdən biri bərpa moduludur (resurrection module). Modul, proqramların tərkibinə plaqin kimi daxil edildikdən sonra zərərli proqramın əsas hissəsi aşkar edilib silindikdə və ya sistemə "patch" tətbiq olunduqda, qrup hədəf sistemə yenidən giriş imkanı əldə edir. Zərərli proqramın digər xüsusiyyəti isə mobil cihazlara giriş funksiyasıdır. Belə ki, bu funksiya vasitəsilə hədəfin mobil cihazından həssas məlumatlar ələ keçirilə bilir. Bununla yanaşı, proqram vasitəsilə "router" və "switch" kimi şəbəkə avadanlıqlarından konfiqurasiya məlumatlarının oğurlanması, daşına bilən disklərdən də silinmiş faylların bərpası baş verə bilər.

Red October qrupunun hücum metodologiyasına gəldikdə ilk növbədə hədəf istifadəçilərə daxilində zərərli fayllar olan e-poçtlar göndərilərək "spear phishing" hücumu həyata keçirilir. Zərərli fayllar əsasən, sistemdəki "MS Word" və "MS Excel" məhsullarındakı boşluqlardan faydalanır.



Qrafik 4. Red October zərərli modullar

Boşluq uğurla istismar olunduqdan sonra hədəf sistem və C2 serveri arasında əlaqə yaranır. Bundan sonrakı prosesdə C2 serverindən zərərli modulların yüklənməsi prosesi həyata keçirirlir. Bu modullar onlayn və oflayn olaraq ayrılır. Modullar işə salındıqdan sonra hədəf sistemdən sistem qeydləri, konfiqurasiya faylları kimi məlumatları toplayır və ya "Adobe Reader" və "Microsoft Office" proqramlarının funksiyalarından istifadə edərək sistemə yenidən giriş əldə edir. Modullar toplanmış məlumatları göndərmək və təlimatları almaq üçün qrupun C2 serveri ilə əlaqə saxlayır.

Silence

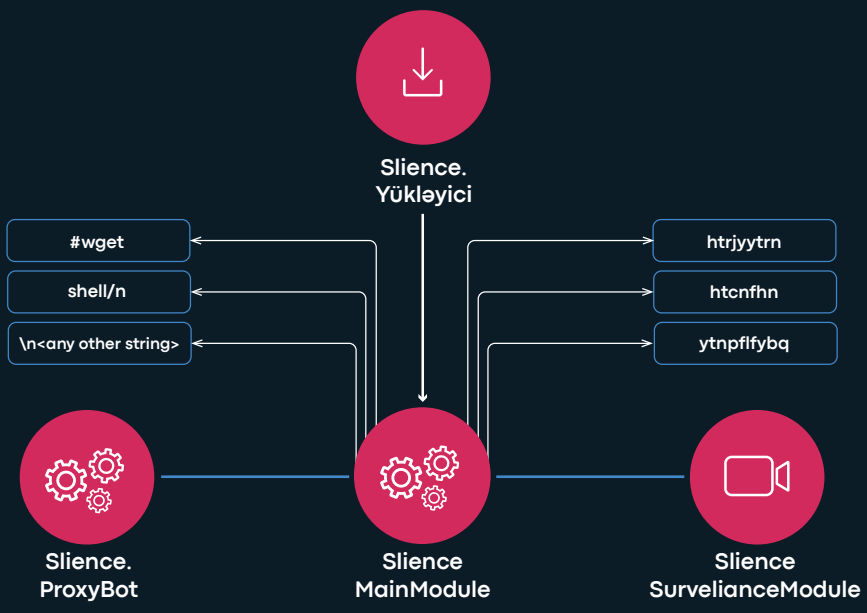
2016-cı ildən fəaliyyət göstərən "Silence" əsasən, bankları hədəf alan və kart məlumatlarını ələ keçirməklə məşğul olan kiber təhdid qrupudur. Qrupun Rusiya federasiyasında yarandığı və fəaliyyət göstərdiyi ehtimal olunur. "Whisper Spider" adı ilə tanınan qrupun əsas hücum hədəfləri təhsil, maliyyə, səhiyyə və sosial sahələrdir. Qrupun hücum etdiyi ölkələr sırasına Rusiya, Ukrayna, Belarus, Azərbaycan, Polşa, Banqladeş və Qazaxıstan və s. daxildir.
Silence-in ən böyük hücum əməliyyatlarından biri 2019-cu ilin may ayında Banqladeşdə yerləşən "Dutch-Bangla Bank"ın bankomatlarına olub. Bu əməliyyatda qrup bankın bankomat şəbəkəsindən istifadə edərək təxminən 3 milyon dollar oğurlamışdır.

Qrupa aid CVE-lər:

CVE-2023-27350, CVE-2023-27351, CVE-2022-3602, CVE-2022-3786, CVE-2022-3199, CVE-2022-31199, CVE-2023-34362

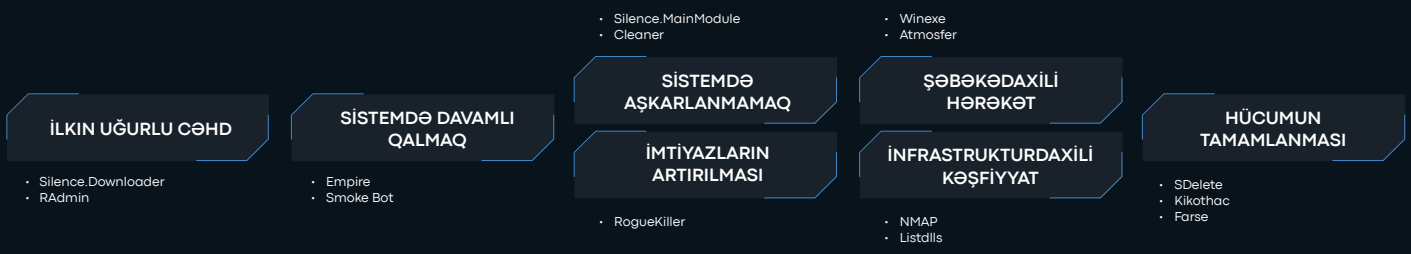
Qrupun hücum metodologiyası

İlk olaraq hədəfə zərərli qoşma ilə təchiz olunmuş fişinq e-poçtu göndərilir. Qoşmanın daxilində "macro" olan "Microsoft Office" sənədi mövcuddur. Hədəf qoşmanı açarsa, sistemə "Silence.Downloader" adlı zərərli proqram yükləyicisi endirilir. "Silence.Downloader" faylı yoluxmuş sistem haqqında məlumatı C2 serverinə göndərir. Bundan sonra qrup növbəti mərhələni manual yükləmək üçün əmr göndərib-göndərməməyə qərar verir. Qrup tərəfindən "Silence.Downloader" zərərli proqram yükləyicisi hədəf sistemə yükləndikdən sonra özünü "startup"a əlavə edir.



Qrafik 5. Silence yoluxma zənciri

Əgər sistem qrup üçün əhəmiyyət kəsb edərsə, əsas zərərli proqram sistemə yüklənilir, əks halda özünü məhv etmə əmrini icra edir. Əsas funksiyası uzaqdan əmrləri yerinə yetirmək və əlavə proqramlar yükləmək olan "Silence.MainModule" adlı zərərli proqram, sistemə əlavə olunduqdan sonra özünü "startup"a əlavə edir. "Silence.MainModule", C2 əlaqələrini təmin etmək üçün "Silence.Proxybot" zərərli modulunu və sistemlərin fəaliyyətlərini izləmək üçün ekran görüntüləri alaraq "Silence.SurvelianceModule" modulunu quraşdırır.



Silence qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

Smoke Bot - Brauzerlər, e-poçt və FTP kimi əlaqə vasitələri üzərindən istifadəçi məlumatlarının toplanması, məlumatlara müdaxilə, real vaxt rejimində şifrlərin ələ keçirilməsi, seçilmiş meyarlar əsasında faylların toplanması və kriptovalyuta mədənçiliyi modullarını əhatə edən geniş spektrdə hücum və kəşfiyyat imkanları təqdim edən alətdir.

Atmosfer - Qrup tərəfindən bankomatları hədəf almaq üçün istifadə edilən mürəkkəb zərərli proqramdır. Proqram zaman keçdikcə inkişaf etdirilərək müxtəlif ATM modellərinə görə uyğun hala gətirilmişdir. Zərərli proqram bankomatın "fwmain32.exe" prosesinə DLL-i yeridir və sistemi uzaqdan idarə etməyə imkan verir. Proqram xüsusi adlandırılmış fayllar vasitəsilə əmrləri qəbul edir və icra edir. Daha sonra ekspertlərin tapmasını çətinləşdirmək üçün həmin faylın daxilinə təsadüfi sözlər yazaraq onu silir.

Cleaner - Uzaqdan bağlantı vasitəsilə sistem qeydlərini, müvəqqəti faylları, log-ları silmək üçün istifadə olunan alətdir.

Inception framework

2017-ci ildən fəaliyyət göstərdiyi ehtimal edilən qrup, kommunal xidmət göstərən müəssisələrə, müdafiə və aerokosmik sektorlara, həmçinin media qurumlarına, səfirliklərə, maliyyə institutlarına və təşkilatlara hücum etməklə tanınır. "Cloud Atlas" kimi də tanınan qrupun hansı ölkə ilə əlaqəli olduğu məlum deyil. Qrupun hədəf aldığı ölkələr sırasına Əfqanıstan, Ermənistan, Azərbaycan, Belarusiya, Belçika, Çexiya, Yunanıstan, Hindistan, İtaliya, Qazaxıstan, Keniya, Malayziya, Moldova, Rusiya Federasiyası, Sloveniya, Cənubi Afrika Respublikası, Türkmənistan, Ukrayna, Böyük Britaniya, ABŞ, Vyetnam daxildir.

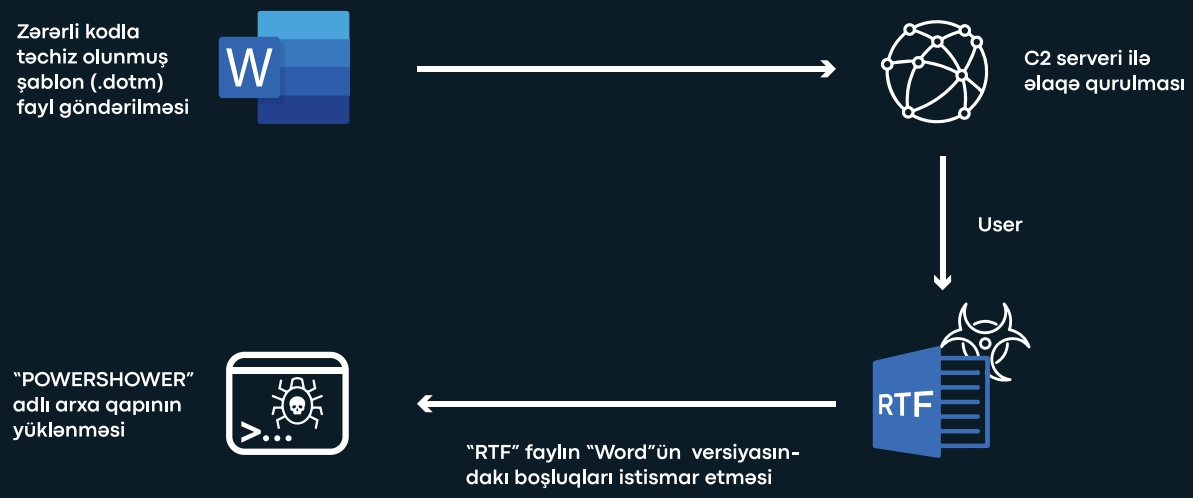
Inception framework qrupu 2021-2023 -cü il tarixlərində Rusiya və Ukrayna arasında gərginliyin artması fonunda hücumlarını Krım yarımadasına və Ukraynanın separatçı bölgələrinə, Luqansk və Donetskə, habelə Rusiyanın hökumət, diplomatik, tədqiqat və sənaye qurumlarına yönəltmişdir.

Qrupa aid CVE-lər:

CVE-2018-0802, CVE-2017-11882

Qrupun hücum metodologiyası

İlk olaraq hədəf istifadəçiyə tərkibində zərərli kodla təchiz olunmuş şablon (.dotm) fayl göndərilir. Fayl açıldığı zaman zərərli şablon faylı yüklənərək C2 serveri ilə əlaqə saxlayır.



Qrafik 6. İnception Framework yoluxma zənciri

C2 serveri ilə əlaqə qurulduqdan sonra istifadəçinin istifadə etdiyi Microsoft Word proqramının versiyası və IP ünvanı növbəti hücum üçün uyğun olarsa, ikinci zərərli "RTF" faylı yüklənmiş olur.
RTF faylı Word mətn prosessorunun köhnə versiyasındakı boşluqları istismar edərək "POWERSHOWER" adlı backdoor-u yükləyir. Nəticədə sistemə sızan qrup C2 serverinə məlumat göndərmə, izləri silmə və daha mürəkkəb zərərli proqram yükləmək kimi fəaliyyətləri həyata keçrir.

Inception Framework qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

PowerShower - Məlumat ötürmək və əlavə təlimatlar almaq üçün "HTTP GET" və "POST" sorğuları vasitəsilə komanda və idarəetmə (C2) serverləri ilə əlaqə saxlamağa kömək edən alətdir. Həmçinin "7Zip"dən istifadə edərək həssas faylları (.txt, .pdf, .xls və .doc) sıxışdırır və çıxarır. Alət registr çalıştırma açarı vasitəsilə yoluxmuş sistemdə davamlılığı təmin etmək və "VBScript"i yerinə yetirmək üçün müxtəlif funksiyalara malikdir. Bundan əlavə C2 kommunikasiyalarını "base64" vasitəsi ilə şifrələyir.

VBShower - HTTP üzərindən C2 serverlərindən VBS skriptlərini qəbul edir və sistemdə davamlılığı qorumaq üçün "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" altında registr qeydləri yaradır. VBShower, VBScript fayllarını yükləmək və icra etmək qabiliyyətinə malikdir. Müvəqqəti İnternet Faylları (Temporary Internet Files) qovluqlarındakı faylları silməklə ekspertlərin işlərini çətinləşdirə bilər.

LaZagne - Əsasən Windows mühitlərinə diqqət yetirir, eyni zamanda Linux və OSX-i dəstəkləyir. LaZagne, RAM, verilənlər bazası, poçt, WiFi, macOS Keychains, Google Chrome, Internet Explorer və Firefox kimi veb brauzerlər də daxil olmaqla, geniş çeşidli mənbələrdən istifadəçi məlumatlarını çıxara bilər.

Cozy Bear

Cozy Bear 2008-ci ildən fəaliyyət göstərən, Rusiya Xarici Kəşfiyyat Xidməti (SVR) ilə bağlı olduğu iddia edilən kiber təhdid qrupudur. Qrupun hədəf aldığı ölkələr sırasına Azərbaycan, Yunanıstan, Ruminiya və İtaliya daxildir. "APT29", "IRON RITUAL", "IRON HEMLOCK", "NobleBaron", "Dark Halo", "StellarParticle", "NOBELIUM", "UNC2452", "YTTRIUM", "The Dukes", "CozyDuke", "SolarStorm", "Blue Kitsune", "UNC3524" adları ilə tanınan qrupun əsas hücum hədəfləri kommunal xidmət göstərən müəssisələr, maliyyə, milli təhlükəsizlik və telekommunikasiya qurumlarıdır.

Cozy Bear qrupu 2023 -cü ildə "Microsoft 365" istifadəçisi olan müəssisələrə hücumlar həyata keçirmək üçün "Microsoft" şirkətinin domenlərinə oxşar domenləri almışdır. Daha sonra istifadəçilərə saxta "Microsoft 365" məhsul keçidləri göndərərək istifadəçi giriş məlumatlarını əldə etməyə çalışmış və bəzi hallarda da buna nail olmuşdur.

Qrupa aid CVE-lər:

CVE-2019-1653, CVE-2019-0859, CVE-2022-24527, CVE-2021-40449, CVE-2022-41120, CVE-2017-11882, CVE-2019-7609, CVE-2018-13379, CVE-2022-26138, CVE-2019-19781, CVE-2022-42475, CVE-2021-26855, CVE-2021-2307, CVE-2023-38831, CVE-2022-30190.

Qrupun hücum metodologiyası

Sağdakı nümunədə qrupun istifadəçilərin e-poçt hesablarına daxil olmaq və zərərli proqram təminatını quraşdırmaq üçün "spear-phishing" və sosial mühəndislik hücumları zamanı istifadə etdiyi fayl təsvir olunub.


DIPLOMATIC CAR FOR SALE

BMW | F10 5 Series Sedan 528i xDrive

Price	:	28.000 EUR
Year	:	2016
City	:	Ankara
Brand	:	BMW
Model	:	5 Series
Km	:	115000 KM
Fuel type	:	Benzin
Engine Power	:	258 hp
Color	:	Grey
Body Style	:	Sedan
Transmission	:	Automatic
Cylinder Volume	:	2000 cm³ (cc)
Specifications	:	ABS, Locks, Alarms, Driver Airbag, Passenger Airbag, Fog Shadow, Leather Seats

Şəkil 2. "DIPLOMATIC-CAR-FOR-SALE-BMW.PDF" zərərli fayl

Qrafik 7. Cozy Bear yoluxma zənciri

Qrafik 7-də qrup ilk olaraq "HTML smuggling" texnikasına əsaslanan "Rootsaw" adlı alətdən istifadə edərək, fişinq e-poçtları vasitəsi ilə "IMG" və ya "ISO" faylını hədəfə göndərir. "HTML smuggling", təhlükəsizlik tədbirlərindən yayınmaq və zərərli məzmunu çatdırmaq üçün istifadə olunur. "ISO" və "IMG" faylının tərkibində "Beatdrop" adlı zərərli fayl və onu icra etmək üçün "LNK" faylı mövcuddur. "BEATDROP" faylı sistem məlumatlarını toplamaq və toplanmış məlumatları C2 serverlərinə göndərmək, fayllar yaratmaq kimi xüsusiyyətlərə malikdir. Qrup C2 əlaqələrinin qurulması üçün "Trello" proqramından istifadə edir. "Trello" proqramının təyinatı tapşırıqların və layihələrin idarə edilməsidir.

Cozy Bear qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

AADInternals - "Azure Active Directory" üzərində əməliyyatlar aparmaq üçün "PowerShell" əsaslı framework-dür. AADInternals (Alət) "Azure AD" istifadəçilərini və cihazları qeydə ala bilir, Azure virtual maşınlarında VM agenti vasitəsilə əmrləri icra edə bilir, həmçinin, "Office 365", "Sharepoint" və ya "OpenID" konfiqurasiyaları kimi bulud xidmətləri haqqında məlumatları qeydə almaq qabiliyyətinə malikdir. Bununla yanaşı, yeni "Azure AD" istifadəçiləri yarada, istifadəçinin OneDrive-ından faylları toplaya və ya müxtəlif autentifikasiya sertifikatlarını yaradıb ixrac edə bilir.

MiniDuke – Alət, bir neçə yükləyici və backdoor komponentlərindən ibarətdir, HTTP və HTTPS üzərindən C2 ilə əlaqə qurmaq üçün "DGA" vasitəsilə yeni Twitter URL-ləri üçün istifadə edə bilir və ya hədəf sistemə GIF faylları vasitəsilə backdoor-lar yükləmək qabiliyyətinə malikdir.

WellMail - Zərərli proqram hədəf sistemdən faylları arxivləyə, sistemdən IP adresi, istifadəçi adı kimi məlumatları əldə edə, C2 serverdən alınan skriptləri icra edə bilir. WellMail zərərli proqramı qarşılıqlı TLS (Transport Layer Security) vasitəsilə komanda və idarəetmə (C2) serveri ilə təhlükəsiz əlaqə üçün əvvəlcədən təyin edilmiş müştəri və Sertifikat Təşkilatı (CA) sertifikatlarından istifadə edir.

CozyCar - Zərərli proqram, HTTP vəya HTTPS vasitəsi ilə C2 serverləri ilə kommunikasiya təmin edərək sistem başlanğıcında icra olunmaq üçün özünü registra əlavə etmək, əmrləri icra etmək, Mimikatz və ya NTLM etimadnamə modulları vasitəsilə hədəf sistemin istifadəçi məlumatlarını toplamaq kimi fərqli funksionallıqlara malik modulları yükləyib, icra etmək qabiliyyətinə malikdir.

Turla

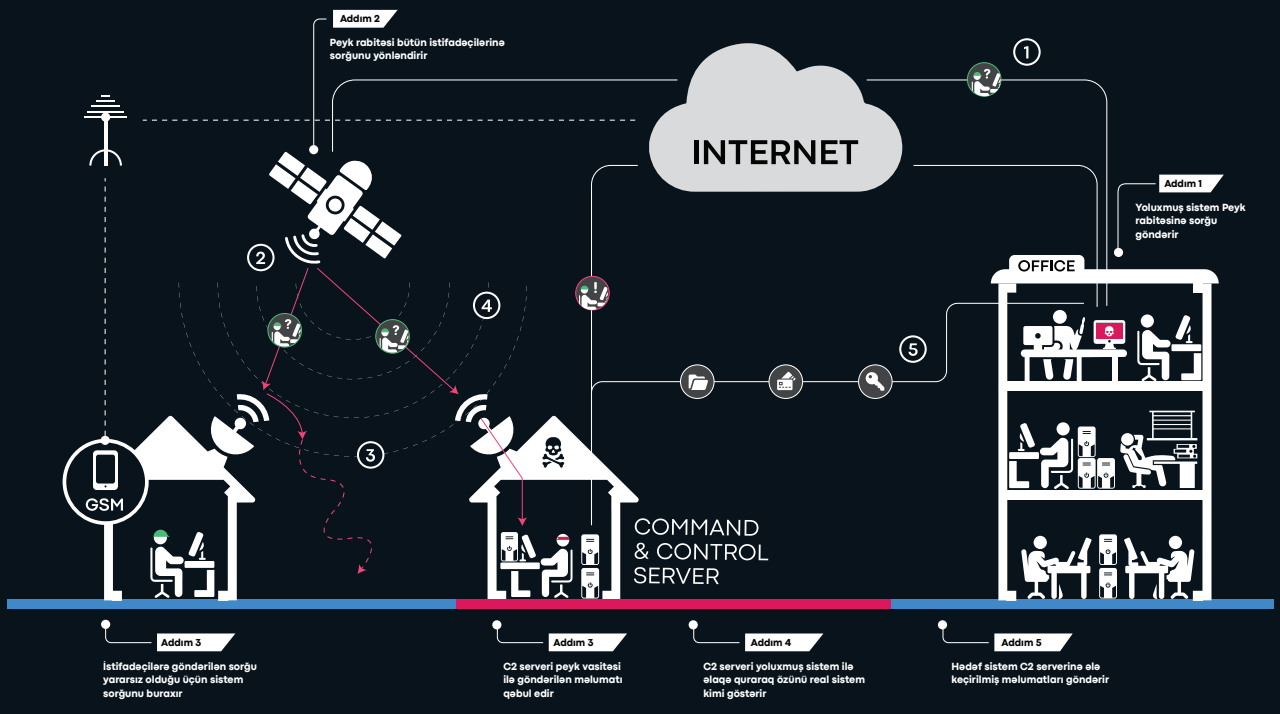
2007-ci ildən fəaliyyət göstərən qrupun Rusiya Federal Təhlükəsizlik Xidməti (FSB) ilə əlaqəli olduğu ehtimal olunur. Qrup Avropa, Yaxın Şərq və ABŞ-da hökumətləri, hərbi təşkilatları və diplomatik qurumları hədəf alması ilə tanınır. "IRON HUNTER", "Group 88", "Belugasturgeon", "Waterbug", "WhiteBear", "Snake", "Krypton", "Venomous Bear" adları tanınan qrupun hücum hədəfləri kommunal xidmət göstərən müəssisələr, dövlət orqanları, istehsalat, səhiyyə, sosial yardım, milli təhlükəsizlik, maliyyə və təhsil qurumlarıdır.

Qrupa aid CVE-lər:

CVE-2022-3236, CVE-2018-0798, CVE-2022-26138, CVE-2022-30190, CVE-2016-0167, CVE-2021-1732, CVE-2016-0165, CVE-2013-3346, CVE-2021-1675, CVE-2018-8453, CVE-2020-0787, CVE-2022-26134, CVE-2022-41107, CVE-2021-28310, CVE-2021-22205

Qrupun hücum metodologiyası

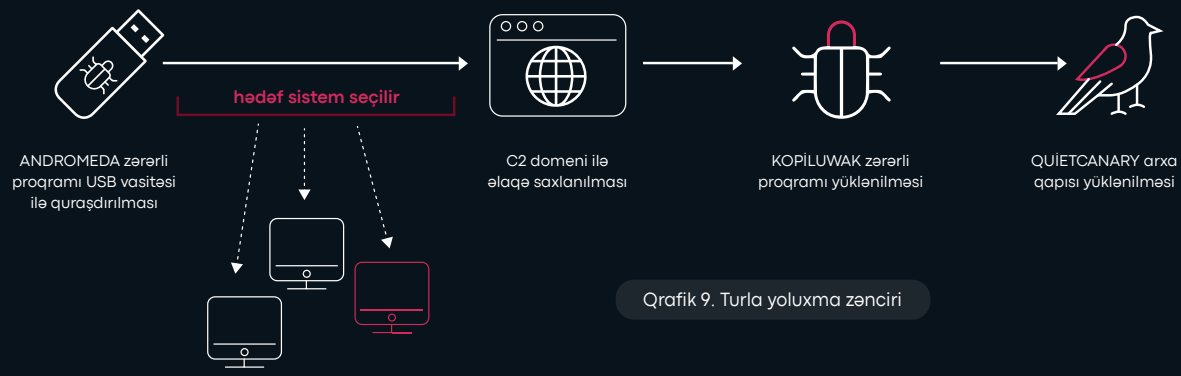
Qrupun 2015-ci ildə zərərli proqramlarına nəzarət etmək və məlumatların çıxarılması üçün peyk rabitə sisteminə sızdığı müəyyən edilmişdir. Qrup, həmçinin peyk internet istifadəçisinin IP ünvanını saxtalaşdıraraq oğurlanmış məlumatları peyk vasitəsilə təhlükəyə məruz qalmış kompüterlərdən digər cihazlara göndərmişdir.



Qrafik 8. Turla yoluxma zənciri

Turla qrupu hücumlarını həyata keçirmək üçün müxtəlif mürəkkəb üsullardan istifadə edir. Bu yanaşmalar onlara yeni zərərli proqram təminatını hədəflərə çatdırmağa imkan verir ki, bu da növbəti hücumlar üçün yeni fürsət yaradır. Turla-nın təşkilatlara ilkin giriş əldə etmək üçün xarici yaddaş qurğuları ilə yayılan zərərli proqramlardan istifadə etdiyi aşkar olunmuşdur.

Bununla yanaşı, qrup hücumlarını həyata keçirmək üçün "ANDROMEDA" adlı zərərli proqramdan istifadə edir. Hücumlarda əsasən, "KOPILUWAK" kəşfiyyat aləti və "QUIETCANARY" backdoor-u kimi vasitələrin birləşməsindən istifadə edir.



Qrafik 9. Turla yoluxma zənciri

"JavaScript" əsaslı köməkçi proqram olan "KOPILUWAK", C2 rabitəsini asanlaşdırır, "QUIETCANARY" isə əsasən, hədəfdən məlumat toplamaq üçün istifadə edilən ".NET" backdoor-udur.

Turla qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

Carbon - Hədəfdən həssas məlumatları oğurlamaq üçün istifadə olunan mürəkkəb, ikinci mərhələ backdoor və framework-dür. Carbon-un arxitekturası onun komponentləri və konfiqurasiya faylını quraşdıran əmrdən, C2 serverləri ilə əlaqə saxlayan və verilən tapşırıqları icra edən və eynilə şəbəkədə olan digər kompüterlərə göndərən orkestratordan ibarətdir.

Gazer - 2016-cı ildən bəri Turla tərəfindən istifadə edilən (Alət), sistemdə gizlilik və davamlılıq üçün hazırlanmış backdoor-dur. HTTP üzərindən kommunikasiya qurur və ".lnk" faylları və qeydiyyat açarları da daxil olmaqla müxtəlif metodlarla öz davamlılığını təmin edir. Gazer, təhlükəsiz C2 kommunikasiyası üçün "3DES" və "RSA" istifadə edərək xüsusi şifrələmə texnikalarından istifadə edir və əməliyyatların gizlədilməsi üçün modullarını internetə açıq proseslərə əlavə edə bilir. Həmçinin tapşırıq icrasını, fayl manipulyasiyasını dəstəkləyir və hərəkətləri şifrələnmiş fayllarda qeyd edə bilir.

Kazuar - "Microsoft .NET" framework-ündən istifadə edilərək inkişaf etdirilmiş, çox platformalı backdoor troyanıdır. Məlumat toplama, "HTTP/HTTPS" və "FTP/FTPS" üzərindən kommunikasiya, həmçinin "cmd.exe" və ya "/bin/bash" vasitəsilə əmr icrası daxil olmaqla geniş funksionallıq dəstəyi təqdim edir. Başlanğıc qovluqlarına və qeydiyyat açarlarına əlavə edilməklə davamlılığını təmin edir və faylları bir C2 serverinə yükləyərək məlumatları sızdıra bilir. Trayan, əlavə plaqinlər yükləyə bilir və aşkarlanmamaq, o cümlədən təhlükəsizlik alətləri tərəfindən müəyyən olunmaması üçün mürəkkəb şifrələmə texnikalarından istifadə edir.

ComRAT - Agent.btz-nin nəsli olduğu ehtimal edilən və 2007-ci ildə ilk tanıdıldığından bəri Turla tərəfindən istifadə edilən mürəkkəb ikinci mərhələ implantıdır. Alət C2 kommunikasiyaları üçün HTTP və e-poçt əlavələrindən istifadə edir. PowerShell vasitəsilə istifadəçi sistemə giriş etdikdə özünü yükləyir və "cmd.exe" vasitəsilə əmrləri icra edir. ComRAT, deşifrələmə üçün hər maşına xüsusi şifrlər və "XOR" açarlarından, HTTP əsaslı C2 kanalı üçün SSL/TLS şifrələməsindən istifadə edir və Gmail üzərindən təhlükəsiz kommunikasiya üçün ictimai açar kriptoqrafiyasından yararlanır. "COM" obyektlərini ələ keçirməklə və qeydiyyat dəyərlərini dəyişdirməklə davamlılığa nail olur. ComRAT-ın gizli əməliyyat qabiliyyəti, gizli fayl sistemi istifadə etmək, virtual fayl sistemini "AES-256" ilə şifrələmək və C2 trafikini maskalamaq üçün modulların sistem proseslərinə, məsələn "explorer.exe" və standart veb brauzerə enjekte etmək kimi xüsusiyyətləri daxildir. Bundan əlavə, əsasən iş saatları ərzində fəaliyyət göstərmək üçün hazırlanmışdır, bu da onu adi şəbəkə fəaliyyətləri ilə daha çox qarışdıraraq gizliliyini təmin edir.

Fancy Bear

"APT28" kimi tanınan Fancy Bear qrupunun müxtəlif mənbələrdə Rusiyanın Hərbi Kəşfiyyat Agentliyi (GRU) ilə əlaqəli olduğu iddia edilir. 2008-ci ildən fəaliyyət göstərən kiber təhdid qrupu ABŞ və Avropada hökumətləri, hərbi təşkilatları və digər yüksək profilli qurumlara kiberhücumlar həyata keçirməsi ilə tanınır. Əsas hədəf aldıqları sahələr milli təhlükəsizlik və dövlət orqanlarıdır. "Fancy Bear" qrupu ən çox fişinq mesajlardan və qurumların rəsmi domen adına oxşar saxta domenlərdən istifadə edərək fərdi məlumatların ələ keçirilməsi ilə məşğuldur. Qrupun hədəf aldığı ölkələr sırasına ABŞ, Kanada, Çili, Azərbaycan, Brazilya, Norveç, Finlandiya, Çin, Yaponiya, Hindistan, Avstraliya və s. daxildir.
Fancy Bear qrupu 2018-ci ilin iyulunda ABŞ Ədliyyə Departamenti Demokratlar Partiyasının Milli Komitəsinin (DNC) serverlərinə hücum və ABŞ seçkilərinə müdaxilə ilə ittiham edilir.

Qrupun istifadə etdiyi zərərli proqramlar:

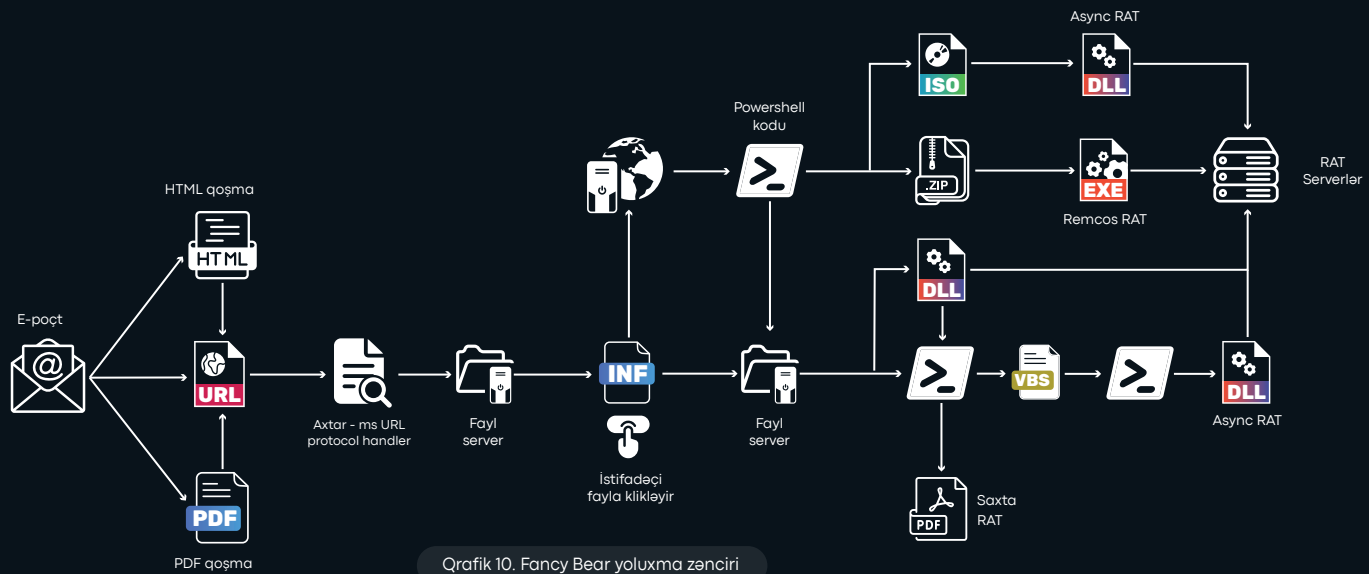
win.karagany, win.cannon, win.caddywiper, komplex, win.mocky_lmk, Raas, NetCode, LoJax, credomap, coreshell, Winexe, driveocean, downdelph, xtunnel_net, Storm-0978, seduploader, oldbait, win.arguepatch.

Qrupa aid CVE-lər:

CVE-2023-23397, CVE-2021-1675, CVE-2021-21551, CVE-2018-8174, CVE-2022-47966, CVE-2021-2307, CVE-2022-26138, CVE-2017-11882, CVE-2022-42475, CVE-2021-35211, CVE-2023-36884, CVE-2022-24527, CVE-2017-6742, CVE-2021-34527, CVE-2021-22205, CVE-2023-38831, CVE-2021-4034, CVE-2021-33764, CVE-2022-30190, CVE-2020-35730, CVE-2019-16098, CVE-2021-44515, CVE-2023-5631, CVE-2020-1472.

Qrupun hücum metodologiyası

Qrup HTML və PDF fayllarından istifadə edərək e-poçt vasitəsilə fişinq hücumuna başlayır. E-poçtun daxilində zərərverici ilə təchiz olunmuş qoşma fayl mövcuddur. İstifadəçi qoşmaya kliklədikdə "search-ms URİ protocol handler"dən istifadə etmək üçün "JavaScript" skripti işə salınır ."Search-ms URI protocol handler" qrupa uzaq hostlarda yerləşən fayl paylaşımları üzrə sorğuların icrasına imkan verir.



Qrafik 10. Fancy Bear yoluxma zənciri

Növbəti mərhələdə LNK faylı yüklənir və faylın açılması "PowerShell" skriptinin icrasına gətirib çıxarır. Bu skript daha sonra ISO, ZIP, EXE , DLL və VBS kimi zərərli faylları və "decoy" PDF faylı fayl serverindən yükləyir. Hədəf istifadəçini aldatmaq üçün yaradılan "decoy" PDF faylının açılması ilə VBS faylları "PowerShell" kodunu icra edir . Bu fayllar (ISO, ZIP, EXE , DLL, VBS) qrupa yoluxmuş sistemi uzaqdan idarə etməyə imkan verən "Async RAT" və "Remcos RAT"ın icrası üçün şərait yaradır. RAT şifrələnmiş kanallardan istifadə edərək qrupun C2 serverləri ilə əlaqə qurur və əmrlərin göndərilməsinə, yoluxmuş cihazı idarə etməyə imkan verir.

Fancy Bear qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

JHUHUGIT - Fancy Bear tərəfindən əsasən kəşfiyyat məqsədləri üçün istifadə edilən və "Carberp" mənbə kodundan törəmiş zərərli proqramdır. HTTP və HTTPS vasitəsilə C2 serverləri ilə əlaqə qurur. Qeydiyyat run açarları və xidmət qeydiyyatı vasitəsilə davamlılıq qurur və məlumat sızdırma , sistem məlumatlarını toplama kimi müxtəlif metodlardan istifadə edir. Proqram "COM" obyektlərinin ələ keçirilməsi, CVE ekspluatları vasitəsilə imtiyazların artırılması kimi texnikalardan və XOR alqoritmləri ilə qarışıqlıqdan yararlanır. "JHUHUGIT"in variantları ekran görüntüsü alma, fayl silmə, əlavə yükün əldə edilməsi (payload) və proses siyahısının alınması qabiliyyətinə malikdir.

Koadic - Windows üçün "zerosum0x0" tərəfindən yaradılan və GitHub-da mövcud olan açıq mənbəli istismardan sonrakı addımlarda istifadə olunan alətdir. Alət Python-da yazılmışdır. Daşına bilən diskə yazıla bilən və ya birbaşa yaddaşa uyğunlaşdırıla bilən JScript və VBScript yükləri yarada bilər. Onun imkanlarına iş masasına uzaqdan giriş, əmrlərin icrası, SMB vasitəsilə faylların ötürülməsi, Mimikatz istifadə edərək etimadnamənin oğurlanması, port skan edilməsi və sistem məlumatlarının toplanması daxildir. Alət, həmçinin xüsusi sistem məlumatlarını və hədəflənmiş faylları toplaya bilər.

XTunnel - VPN-ə bənzər şəbəkə proksi alətidir. Həmçinin tədqiqatlar zamanı məlum olmuşdur ki, zərərli proqram yerli olaraq saxlanılan şifrlərə girişi dəstəkləyir və LDAP serverə daxil ola bilir. C2 serveri ilə hədəf arasında trafikin yönləndirilməsini təmin edir, trafiki SSL/TLS və RC4 ilə şifrələyir. XTunnel, şəbəkələri araşdırma, uzaqdan əmrlər icra etmə və yerli saxlanılan şifrlərə giriş qabiliyyətinə malikdir. Qarışıqlıq texnikalarından istifadə edir və port nömrələrini dəyişərək şəbəkə şəraitinə dinamik olaraq uyğunlaşmaq üçün davamlılıq təmin edir.

XAgentOSX - OS X sistemlərini hədəfləyən mürəkkəb troyandır. Troyan, "OS X" üçün uyğunlaşdırılmış "CHOPSTICK" və ya "XAgent" troyanının bir versiyası hesab edilir. Zərərli proqram, FTP vasitəsilə faylları yükləmə, Firefox şifrlərini əldə etmə, qovluq məzmununu siyahıya alma, iOS cihaz yedəklərini yoxlama, faylları silmə, klaviatura vurğularını qeyd etmə, faylları icra etmə, prosesləri siyahıya alma, ekran görüntüləri alma, quraşdırılmış tətbiqləri müəyyən etmə və sistem versiyası və istifadəçi məlumatlarını toplama qabiliyyətləri daxil olmaqla, bir çox funksiyalara malikdir. Bu funksiyalar XAgentOSX-i casusluq və məlumat sızdırmaq üçün çox yönlü proqrama çevirir.

Gananite

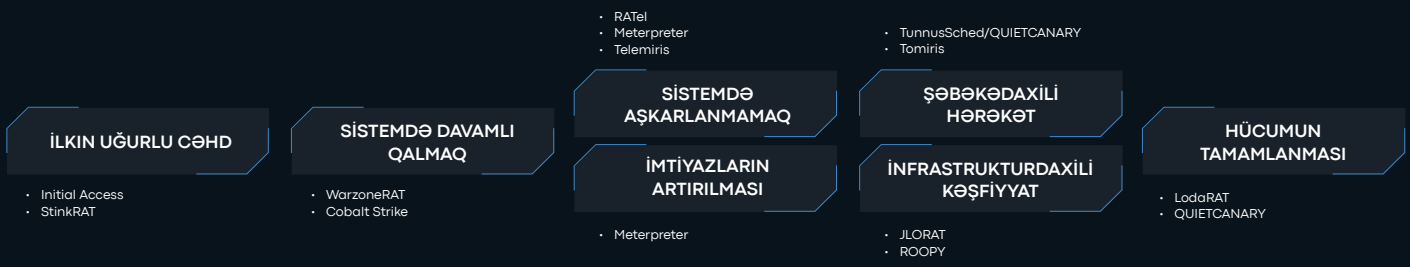
Qrupun hansı ölkəyə məxsus olması ilə bağlı rəsmi qaynaqlarda məlumat qeyd olunmamışdır. Müstəqil Dövlətlər Birliyində və Mərkəzi Asiya ölkələrində hücumlarını həyata keçirən "Gananite" qrupunun əsas hücum hədəfləri neft, qaz, nəqliyyat şirkətləri və dövlət qurumlarıdır.

Qrupa aid CVE-lər:

CVE-2019-12593, CVE-2020-25925, CVE-2021-36260, CVE-2019-11510, CVE-2020-8515, CVE-2020-14472, CVE-2022-24500, CVE-2022-0848, CVE-2022-22972, CVE-2021-44158, CVE-2022-26809, CVE-2022-30190, CVE-2022-26937, CVE-2022-30136, CVE-2022-1388, CVE-2022-30075, CVE-2022-24086, CVE-2021-42013, CVE-2019-9193

Qrupun hücum metodologiyası

"Gananite" qrupu hədəf sistemə hücum etmək üçün əsasən fişinq metodlarından istifadə edir. Bunun üçün qrup, hədəf şirkətin istifadə etdiyi domen adlarının bənzərlərini yaradır və "spear-phishing" metodundan istifadə edərək, hədəfin məlumatlarını ələ keçirir. Bununla yanaşı qrupun "pdf", "lnk", "hta" və "vhdx" formatlı zərərverici faylları da bənzər texnikalar vasitəsilə hədəfə göndərdiyi müşahidə edilmişdir.



Gananite qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

WarzoneRAT9 – Eksperlər tərəfindən aşkarlanmamaq imkanları olan və məlumat oğurluğunda istifadə olunan troyandır.

Telemiris - Telegram-dan C2 kanalı kimi istifadə edən Python backdoor-udur.

JLORAT - Məlumatların toplanması və C2 serverinə ötürülməsi üçün istifadə edilən zərərli proqramdır.

ROOPY - Paskal əsaslı zərərli proqram, şəbəkəni skan edə və məlumatları C2 serverinə göndərə bilir.

Stibnite

2019-cu ilin sonundan bəri bilinən "Stibnite" ICS sistemlərini və dövlət qurumlarını hədəf alan kiber təhdid qrupudur. Əsas hücum hədəfləri neft, qaz şirkətləri, kommunal xidmət göstərən müəssisələr və dövlət qurumlarıdır. Qrupa aid CVE-lər barədə məlumatlar əldə olunmamışdır.

"Stibnite" qrupu 2021-ci ildə Azərbaycanda enerji sektorunu hədəf almışdır. Əsas hücum vasitəsi olaraq sosial mühəndislik metodlarından istifadə etmişdir. Belə ki, hədəfə içində zərərli kod gizlədilən "Ms Office" sənədini göndərən qrup, müxtəlif üsullardan istifadə edərək hədəfin faylda "macro" funksiyasını aktivləşdirməsinə məcbur edir. "Macro" funksiyasını aktivləşdikdən sonra isə əsas zərərverici proqram sistemə yüklənir və sistemdəki vacib məlumatların əldə edilməsi prosesi başlanılır.


SOCAR

25 Mart 2021
Azərbaycan Respublikasının
Ekologiya və Təbii Sərvətlər nazirliyinə

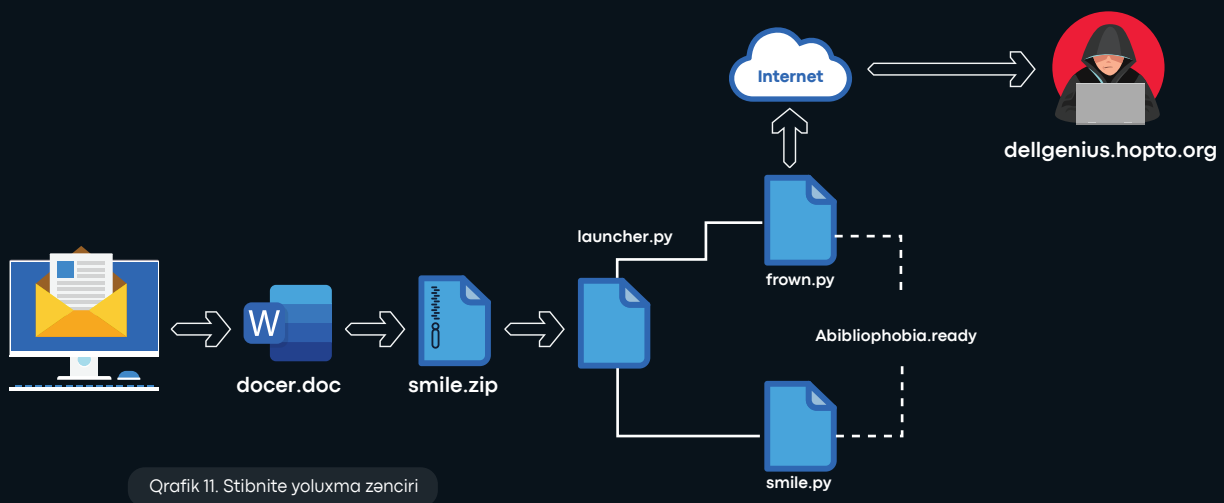
Heydər Əliyev adına
Neft Emalı Zavodu
0 Vəliyev küç. 1
AZ 1060, Azərbaycan, Bakı
Tel.: (994 12) 521 23 21
Tel.: (994 12) 521 23 19
Faks: (994 12) 521 23 03
e-mail: office.haor@socar.az

Katalizatorun analiz olunması üçün ixraca göndərilməsi haqqında

Şəkil 3. Ms Office sənədi

Qrupun hücum metodologiyası

Qrafik 11-də "Stibnite"in hücum metodologiyasına nəzər yetirsək, ilk olaraq daxilində macro olan "Microsoft Word" sənədi (docer.doc) hədəf cihaza müxtəlif üsullar ilə yüklənilməyə çalışır. Zərərli "VBA" kodu "simle.zip" adlı faylı yaradır.



Qrafik 11. Stibnite yoluxma zənciri

Zip faylı istifadəçi tərəfindən açıldıqda "launcher.py" adlı "python" faylı icra olunur. "launcher.py" ilk əvvəl diskin ölçüsünü yoxlayır, sonra digər iki "python" faylını icra edir (smile.py, frown.py). Fayllardan "Smile.py" əmrləri, nəticələri, məlumatları saxlayan və məzmunu "Affine" şifrəsi şəklində şifrələnmiş fayl (Abibliophobia23.ready) yaradır. "Frown.py" faylı isə qrupun serveri ilə əlaqə quraraq onun tərəfindən verilən əmrləri "Abibliophobia23.ready" faylında saxlayır. Bu əmrlərə fayl yükləmək, registr redaktə etmək və s. kimi bir çox funksiyalar daxildir.

Stibnite qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

PoetRAT – Python və Lua proqramlaşdırma dilləri ilə yazılmış uzaqdan qoşulma troyanıdır (RAT). Troyan cihazları uzaqdan idarə etmək, məlumatları oğurlamaq və digər əməliyyatları yerinə yetirmək üçün istifadə edilir. C2 əlaqələri üçün HTTP, HTTPS, FTP və ya digər xüsusi protokollardan istifadə edə bilər.

WinPwnage – İmtiyazları artırmaq, sistemdə davamlılığı təmin etmək, İstifadəçi Hesabına Nəzarətdən (UAC) yan keçmək, prosesləri manipulyasiya etmək və ixtiyari kodu icra etmək üçün müxtəlif Windows zəifliklərindən və xüsusiyyətlərindən istifadə etməyə yönəlmiş alətdir.

Dog.exe – ".NET" vasitəsilə yazılmış cihazdakı fərdi məlumatları e-poçt və ya "FTP" vasitəsilə oğurlamağa çalışan zərərli proqramdır.

Browdec.exe - Brauzer tarixçəsini, saxlanılan şifrləri və sessiyaları oğurlamaq üçün istifadə olunur.

Soleimani Cyber Army

İran İslam Respublikası ilə əlaqəli olduğu güman edilən qrupun əsas hücum hədəfləri təhsil, telekommunikasiya müəssisələri və dövlət qurumlarıdır. "Soleimani İranian Cyber Army" qrupunun əsas məqsədi dövlət qurumlarına aid sistemləri ələ keçirərək siyasi mövzularda məzmun paylaşmaqdır. Qrup, 2023-cü ilin aprel ayında Azərbaycanın bir sıra internet resurslarına hücumlar təşkil etmişdir. Həmçinin müxtəlif vaxtlarda kiber təhdid qrupu tərəfindən Azərbaycanda özəl sektora məxsus informasiya sistemi və şəbəkələrinə də hücumlar həyata keçirilmişdir.

Soleimani İraninan Cyber Army qrupunun Azərbaycan veb resurslarına etdiyi hücuma nümunə

Əsas hücum metodu olaraq veb resurslarda istifadə olunan yenilənməmiş və müəyyən boşluqlara sahib proqram təminatlarından istifadə edilmişdir. Kiber kəşfiyyat analitiklərindən əldə olunan məlumatlara əsasən, "Soleimani İraninan Cyber Army" kiberhücumlarını "APT 42" adlı təhdid qrupu ilə birlikdə həyata keçirmişdir.

Qrupa aid CVE-lər:

CVE-2020-7109, CVE-2020-7055, CVE-2020-8426, CVE-2020-36171, CVE-2022-46169, CVE-2022-0730, CVE-2020-13126

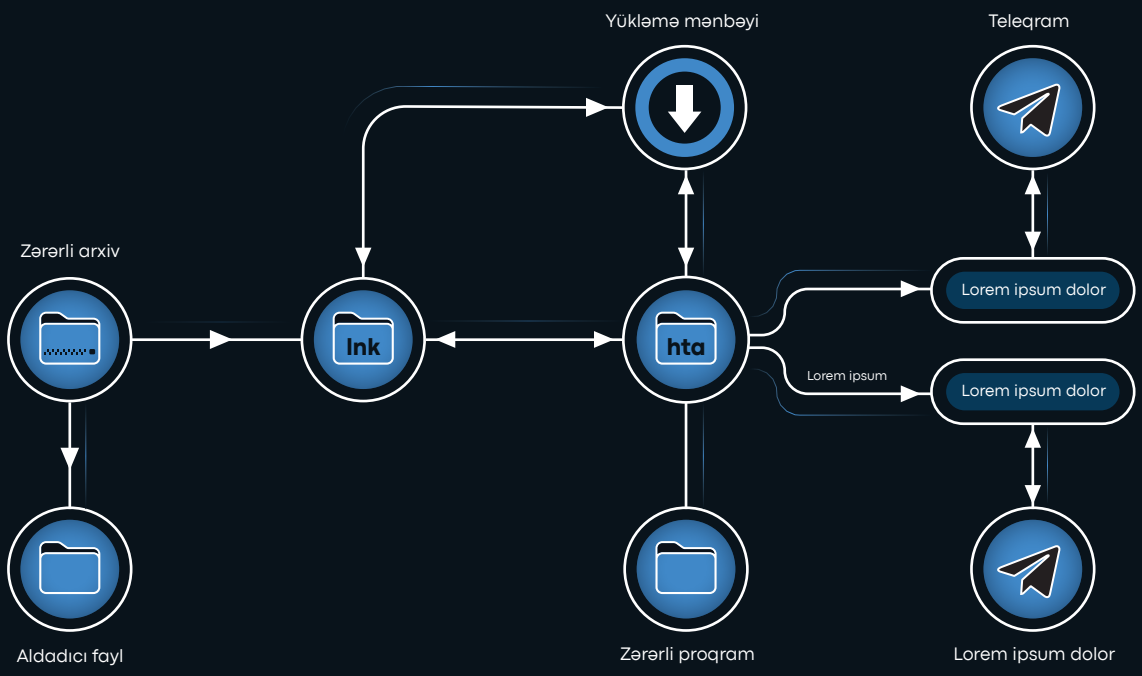
YoroTrooper

2022-ci ildən bu yana tanınan "YorotTrooper" təhdid qrupunun Qazaxıstan respublikası ilə əlaqəli olduğu ehtimal edilir. Qrupun hədəf aldığı ölkələr sırasına Özbəkistan, Tacikistan, Rusiya, Azərbaycan, Belarus daxildir. Əsas hədəf aldıqları sahələr kommunal xidmət göstərən müəssisələr, səfirliklər və dövlət orqanlarıdır.
2022-ci ildə "YoroTrooper" qrupunun Avropa İttifaqı Səhiyyə Agentliyi (EU Health Care Agency) və Ümumdünya Əqli Mülkiyyət Təşkilatı (World Intellectual Property Organization-WIPO) ilə əlaqəli istifadəçi hesablarını sızdırdıqları müəyyən olunmuşdur.

Qrupun hücum metodologiyası

Qrup ilk növbədə hədəfə fişinq mesajı və ya e-poçtlar göndərərək, istifadəçini zərərli əlavəni açması üçün aldatmağa çalışır. Hədəf zərərli əlavəni icra edərsə, cihazına zərərli fayl yüklənir. Bu fayl adətən bir və ya bir neçə zərərli faylı ehtiva edən arxiv faylıdır. Zərərli arxivdə həmçinin "LNK" faylı və ya "HTA" faylı ola bilər. "LNK" faylı başqa bir fayla qısayoldur.

Yoluxma zənciri



Qrafik 12. YoroTrooper yoluxma zənciri

İstifadəçi "LNK" faylına kliklədikdə həmin fayl istinad olunduğu faylı icra edir. "HTA" faylı isə skriptləri işə salmaq üçün istifadə edilən "HTML" faylıdır. İstifadəçi "HTA" faylını açdıqda isə faylda olan zərərli skriptlər icra olunur. Növbəti mərhələdə bu fayllar vasitəsi ilə hədəf cihaza uzaqdan qoşulma troyanı (RAT) kimi zərərli proqramlar yüklənir. Bu proqramlar "telegram" və ya C2 serverləri vasitəsi ilə qrupun sistemə uzaqdan qoşulması, məlumatların oğurlaması kimi bir çox əməliyyatları yerinə yetirməsinə imkan verir.

İLKIN UĞURLU CƏHD	HÜCUMUN TAMAMLANMASI
• WarzoneRat • Loda RAT	• Stink stealer

YoroTrooper qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

Stink stealer - İstifadəçi məlumatları, kukilər və "bookmark" toplayan "Chromium" əsaslı brauzerlərdən bir neçə modullara malik zərərli proqramdır. Discord və Telegram-dan "Filezilla" istifadəçi məlumatlarını və autentifikasiya kukilərini toplayır. Zərərli proqram ekran görüntüsü, IP ünvanı, əməliyyat sistemi, aktiv prosesslər kimi məlumatları ələ keçirə bilər.

WarzoneRat - C++ dilində yazılmış uzaqdan giriş troyanıdır. Troyan hədəf sistemin fayllarını və şifrlərini oğurlamaqdan tutmuş masaüstü fəaliyyətləri ələ keçirməyə qədər geniş imkanları özündə cəmləşdirir. "WarZone RAT", əsasən fişinq e-poçtları vasitəsilə göndərilir və C2 serverindən müntəzəm yeniləmələr alır.

Loda RAT - Windows və Android sistemləri üçün uzaqdan giriş troyanıdır (RAT). Troyanın əsas məqsədi brauzerlərdə saxlanılan istifadəçi adlarını, şifrləri və kukiləri oğurlamaq olsa da o, həmçinin klaviatura qeydi, səs yazma və ekran görüntüsü imkanlarına malikdir.

OilRig

2014-cü ildən fəaliyyət göstərən "OilRig", İranda yerləşdiyi ehtimal olunan kiber təhdid qrupudur. Qrup Yaxın Şərqdə, eyni zamanda ABŞ, Avropa ,Asiya kimi digər bölgələrdə yerləşən təşkilatlara qarşı kiber hücumlar həyata keçirməsi ilə tanınır. "COBALT GYPSY", "IRN2", "APT34", "Helix Kitten", "Evasive Serpens" adları tanınan qrupun əsas hədəf aldıqları sahələr maliyyə sektoru, kommunal xidmət göstərən müəssisələr, dövlət orqanları, kimya, təhsil, neft, qaz, telekommunikasiya, aviasiya şirkətləri və hotellərdir. "OilRig"in hədəf aldığı ölkələr sırasına Oman, Azərbaycan, Bəhreyn, İraq, İsrail, İordaniya, Küveyt, Livan, Qətər, Səudiyyə Ərəbistanı, Cənubi Afrika, Türkiyə, Birləşmiş Ərəb Əmirlikləri, Pakistan, Türkiyə, Böyük Britaniya, ABŞ və s. daxildir.

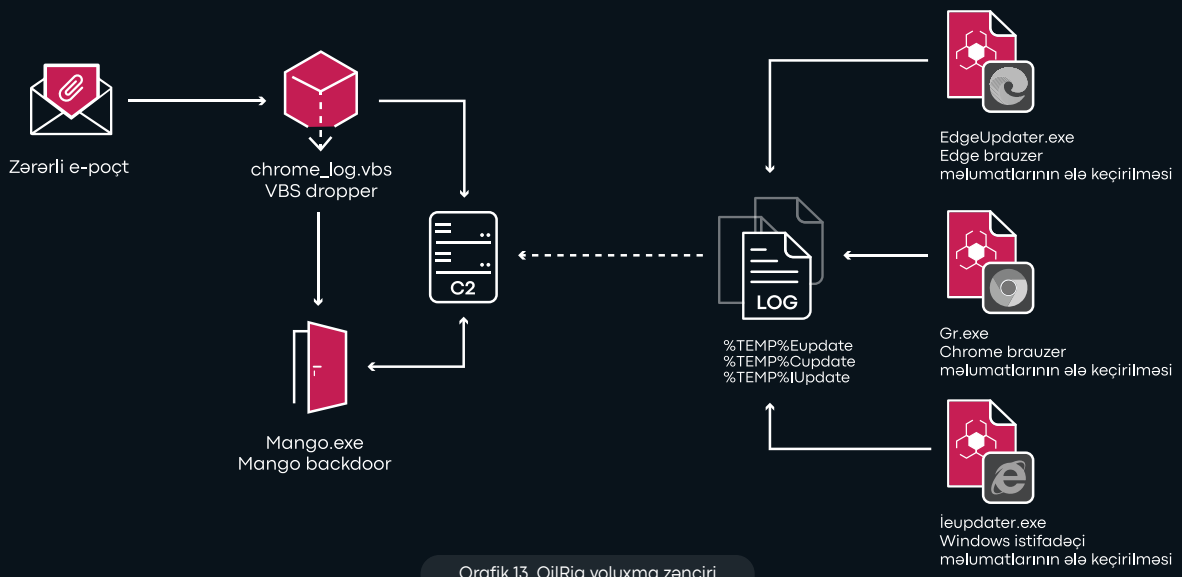
2022-ci ildə "OilRig", İsrail təşkilatlarına qarşı mürəkkəb kiberhücum həyata keçirmişdir. Belə ki, qrup C2 əlaqələri qurmaq üçün zərərli proqramlar vasitəsilə "Microsoft OneDrive" və müxtəlif "Microsoft Qrafik API" kimi qanuni "Microsoft" bulud xidmətlərindən istifadə etmişdir. Qrupun bulud xidmətlərindən istifadə etməsi və yeni zərərli proqramlarının davamlı inkişafı onların taktikalarının yenilənməsinə, davamlı hücumlarını həyata keçirməsinə şərait yaratmışdır.

Qrupa aid CVE-lər:

CVE-2017-11882, CVE-2017-0199, CVE-2017-11774, CVE-2018-0802

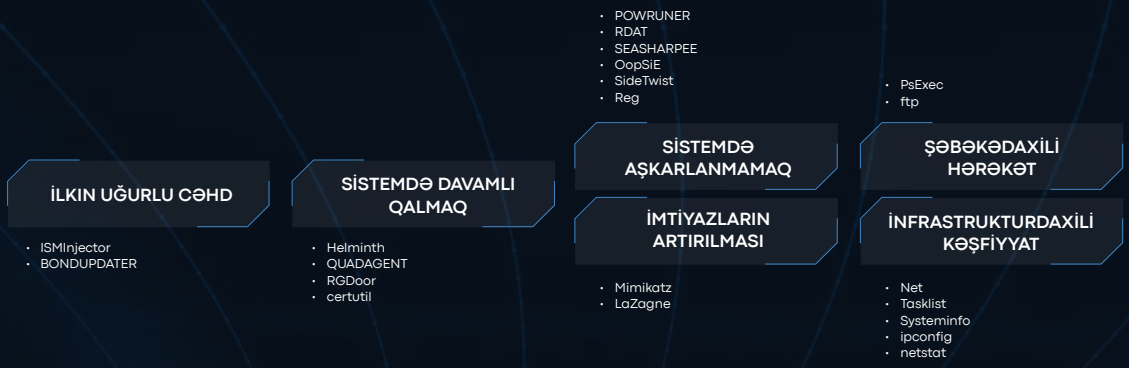
Qrupun hücum metodologiyası

"OilRig" qrupu əsasən "supply chain" hücumlarını həyata keçirir, burada təhdid qrupu təşkilatlar arasındakı bağlantılardan istifadə edərək əsas hədəflərinə hücum edir. Hücumlarında proqram təminatı zəifliklərindən daha çox sosial mühəndislik metodundan istifadə edir. Lakin bəzən qrup zərərli proqramların hədəfə çatdırılması üçün ən son aktiv olan boşluqlardan da istifadə edir.



Qrafik 13. OilRig yoluxma zənciri

Qrafikə nəzər yetirsək qrup, tərkibində "VBScript dropper" (chrome_log.vbs) zərərli proqramı yerləşdirilmiş e-poçt vasitəsi ilə hücuma başlayır. "VBScript dropper"in funksiyası "Mango.exe" backdoor-unu yükləmək, sistemdə qalıcılıq üçün tapşırıqları planlaşdırmaq və C2 serverində qeyd etməkdir. Qrup "mango.exe" backdoor-u ilə əmr və idarəetmə (C2) serverinə qoşulur. Eyni zamanda "Mango.exe" ilə birlikdə sistemə 3 ayrı ".exe" faylı yüklənir (EdgeUpdate.exe, Gr.exe, ieupdater.exe). Yüklənmiş fayllar brauzerdən istifadəçi məlumatları, kukilər, brauzer keçmişi kimi məlumatları və "Windows İstifadəçi Məlumatları Meneceri"ndən (Windows Credential Manager*) isə istifadəçi məlumatlarını oğurlayır və C2 serverə ötürür.



OilRig qrupunun hücum zamanı istifadə etdiyi proqram və alətlər

BONDUPDATER - Powershelldə yazılmış backdoor-dur. Bu zərərli proqram əmr və idarəetmə serveri üçün "DNS tunelling" protokolu daxilində DNS və TXT qeydlərindən istifadə edə bilər. Proqram özünü hər dəqiqə icra etmək üçün tapşırıq planlaşdırılmasından istifadə edir.

RDAT - Sistemə nəzarət və məlumatların ələ keçirilməsi üçün qabaqcıl üsullardan istifadə edən çoxşaxəli zərərverici proqramdır. Proqram, HTTP və DNS vasitəsilə əmr və idarəetmə (C2) serverləri ilə əlaqə saxlayır, gizlilik üçün şifrələmə və steqanoqrafiyadan istifadə edir. RDAT əmrləri yerinə yetirə və zərərli xidmətlər yarada bilər. Proqram, həmçinin aşkarlanmadan yayınmaq üçün özünü silmək kimi bir çox imkanlara malikdir.

SideTwist – Əsas məqsədi C2 əlaqəsini təmin etmək, C2 serveri tərəfindən göndərilmiş əmrləri və ya proqram fayllarını icra etmək və ya sistemdəki faylları C2-yə yükləmək olan troyandır. Troyan, ətraflı sistem məlumatlarını toplamaq və aşkarlanmadan yayınmaq imkanlarına malikdir.

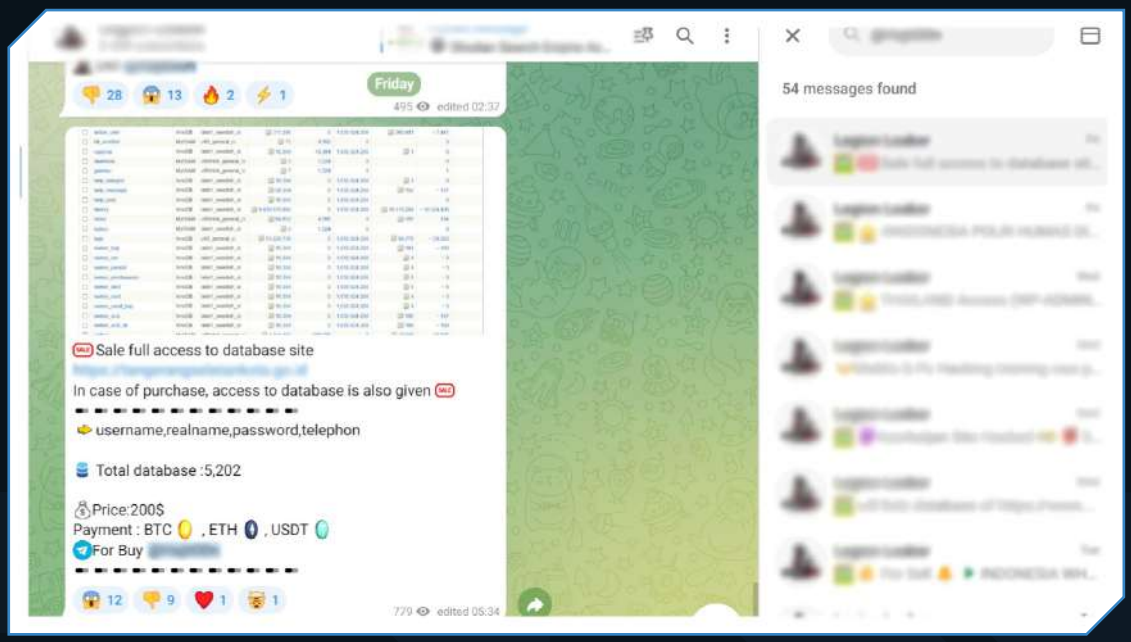
ISMInjector – Sistemdə qalıcılığı təmin etmək üçün planlaşdırılmış tapşırıqlardan istifadə edən backdoor-dur. Faylları deşifrə etmək üçün "certutil" alətindən istifadə edir.

EbRaHIM-VaKeR

İran İslam Respublikası ilə əlaqəli olduğu ehtimal edilən "EbRaHiM-VaKeR" ləqəbli xaker, müxtəlif sferaları hədəf alması ilə tanınır. "EbRaHiM-VaKeR" adətən ələ keçirdiyi veb-saytların ana səhifəsini dəyişdirərək öz teleqram kanalına yönləndirir. Əsas məqsədi ələ keçirdiyi məlumatları və zərərli proqramları satmaqdır. Xaker sızdığı sistemlərdə hər-hansısa siyasi məzmunlu paylaşımlar etmir. Xakerin bu vaxtadək 60-ı Azərbaycan saytı olmaqla 2.500-dən çox veb-saytı "deface" etdiyi məlum olmuşdur.

Şəkil 5. EbRaHiM-VaKeR uyğunsuz kontent

EbRaHiM-VaKeR-in əsəs hücum hədəfi "Wordpress" üzərindən qurulan veb resurslardır. Belə ki, veb resurslarda yaranan boşluqlardan xüsusilə də, qlobal olaraq ümumi axtarış edən proqramlar yazaraq hücumlarını həyata keçirmişdir.



Şəkil 6. EbRaHiM-VaKeR-in Telegram səhifələri

Xakerin müxtəlif vaxtlarda "Delta Security Team", "MiHaNHack Security Researcher Team" və "Iranonymous"un üzvü olduğu aşkarlanıb.

Azərbaycanı hədəf almış

Ransomware qrupları

"SOCRadar" şirkətinin 2021-ci hesabatında Azərbaycan internet informasiya ehtiyatlarına hücum etmiş 3 ransomware" qrupu qeyd olunmuşdur:

LOCKBIT

CONTI

CRING

Lockbit

"Lockbit" qrupu, "LockBit 2.0" və "LockBit 3.0" fidyə proqramlarından istifadə edərək, dünyada minlərlə təşkilatı hədəf almış, müxtəlif taktika, texnika və prosedurlardan istifadə edən yüksək fəal və davamlı inkşaf edən "Ransomware" xidməti (RaaS) verən qrupdur. "LockBit 3.0" fidyə proqramı əvvəllər "Windows", "Linux"və "VMware ESXi" serverlərini hədəfləsə də, "MacOS", "ARM", "FreeBSD", "MIPS" və "SPARC CPU"larına da təsir edə bilən yeni versiyaları müəyyən edilmişdir. "Lockbit" qrupunun əsas hədəf aldıqları sahələr istehsal, səhiyyə, təhsil, İT sahələri, kiçik və orta bizneslərdir.

Qrupa aid CVE-lər:

CVE-2022-26134, CVE-2022-30190, CVE-2017-17215, CVE-2024-1708, CVE-2022-3236, CVE-2022-36537, CVE-2021-44228, CVE-2022-47966, CVE-2023-29324, CVE-2023-38831, CVE-2023-20198, CVE-2023-5009, CVE-2023-22518, CVE-2021-34523, CVE-2020-0787, CVE-2017-0143, CVE-2014-3153, CVE-2021-31207, CVE-2021-34473, CVE-2018-0798, CVE-2021-20028, CVE-2017-0147, CVE-2022-42475, CVE-2021-36942, CVE-2017-11882, CVE-2023-36884, CVE-2021-22986, CVE-2023-20269, CVE-2023-20109, CVE-2023-3519, CVE-2023-46747, CVE-2023-5129, CVE-2023-40044, CVE-2023-46748, CVE-2023-27350, CVE-2023-4966, CVE-2023-46604, CVE-2023-23397, CVE-2024-1709, CVE-2023-38035, CVE-2018-13379, CVE-2015-1650, CVE-2023-22515, CVE-2023-34039, CVE-2017-8464, CVE-2024-21412, CVE-2017-0199, CVE-2023-36025, CVE-2020-0796.

Qrupun hücum metodologiyası

Qrup "RDP" və "VPN" girişi üçün istifadəçi adı və şifrlərinə qarşı kobud güc hücumları (Brutforce) həyata keçirməklə və ya bərpa olunmamış boşluq vasitəsi ilə hədəf şəbəkəyə ilkin giriş əldə edir. Giriş əldə etdikdən sonra hədəfin şəbəkəsi daxilində əmr və idarəetmə sistemləri qururlar.

Qrafik 14. Lockbit yoluxma zənciri

Şəbəkəyə daxil olduqdan sonra digər sistemlərə sızmaq üçün müxtəlif üsullardan istifadə edirlər. Buna daxili "PowerShell" əmrlərindən və ya qrup siyasəti (Group policy) konfiqurasiyalarından sui-istifadə daxildir. Sonda qrup fayl sistemini şifrələmək, faylları əlçatmaz etmək və hədəflərə mesajlarını çatdırmaq üçün fidyə proqramını icra edirlər. Qrup əldə olunan məlumatların geri qaytarılması üçün danışıqları "TOR" şəbəkəsində yerləşdirilən veb portallar vasitəsilə aparır.

Conti

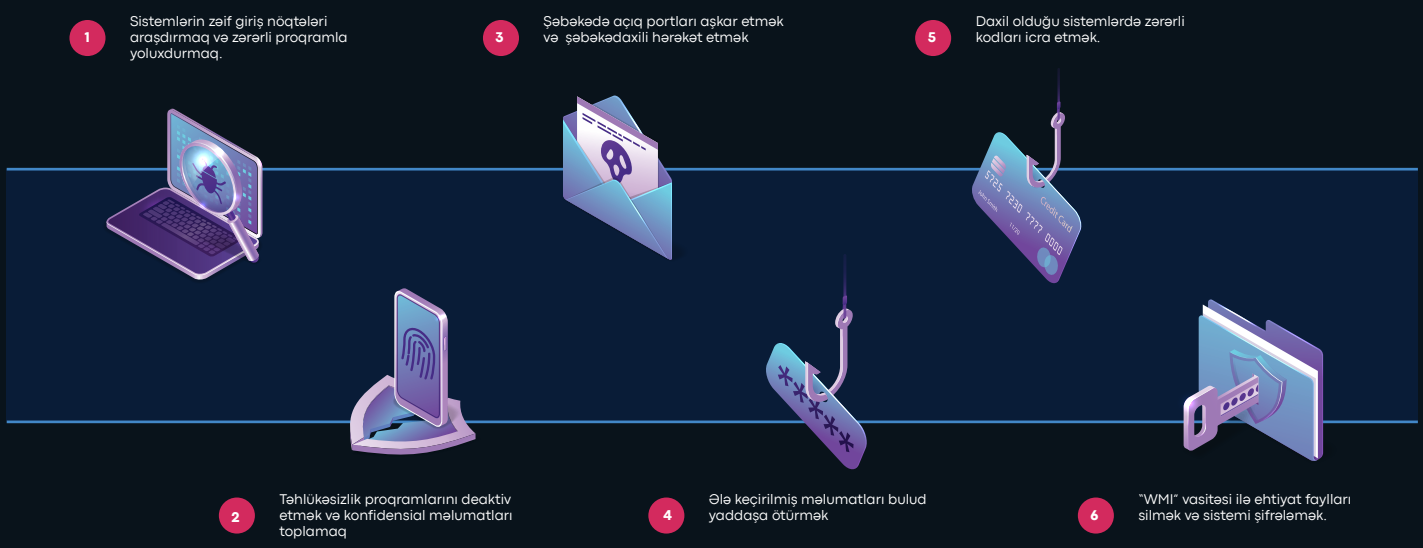
İlk dəfə 2019-cu ildə müşahidə olunan "Conti ransomware" qrupu aktiv və təhlükəli "Ransomware" xidməti (RaaS) göstərən qrupdur. Qrupun dünya üzərində 400-dən çox zərərverici fəaliyyətlə məşğul olduğu təxmin olunur. Əsas hədəf aldıqları sahələr istehsal, səhiyyə və tikinti şirkətləridir.

Qrupa aid CVE-lər:

CVE-2024-1708, CVE-2022-40684, CVE-2022-36537, CVE-2023-23583, CVE-2023-47246, CVE-2021-40539, CVE-2023-22518, CVE-2021-34523, CVE-2020-0787, CVE-2021-31207, CVE-2021-34473, CVE-2023-34051, CVE-2023-3284, CVE-2021-20028, CVE-2023-46850, CVE-2023-23369, CVE-2023-20592, CVE-2021-36942, CVE-2021-22986, CVE-2023-20269, CVE-2023-46747, CVE-2023-46849, CVE-2023-27350, CVE-2023-36033, CVE-2023-46604, CVE-2024-1709, CVE-2018-13379, CVE-2022-42821, CVE-2023-34057, CVE-2023-36036, CVE-2023-23368, CVE-2023-34058, CVE-2023-34048,

Qrupun hücum metodologiyası

Qrup ilk növbədə hədəf sistemlərin zəif giriş nöqtələrini araşdıraraq, onları zərərli proqramlarla yoluxdurmağa çalışır. Növbəti mərhələdə təhlükəsizlik proqramları deaktiv edilərək, konfidensial məlumatlar əldə olunur.



Qrafik 15. Conti qrupunun yoluxma zənciri

Bir sonrakı mərhələ şəbəkədəki açıq portları aşkar etmək və şəbəkədaxili hərəkət etməkdir. Nəticədə ələ keçirilmiş məlumatlar bulud yaddaşa köçürülür və daxil olunan sistemlərdə zərərli kodların icrası baş verir. Son olaraq "WMI" vasitəsi ilə ehtiyat fayllar silinir və sistem şifrələnir.

Cring

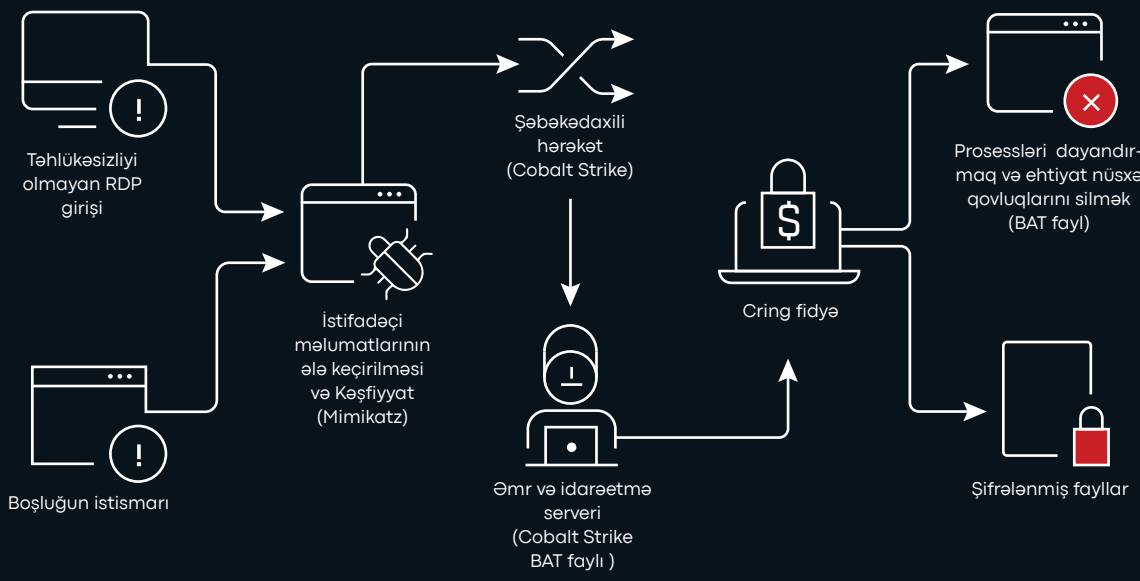
"Cring" qrupu ilk dəfə "Adobe ColdFusion"da olan xətadan istifadə edərək tanınmışdır. Əsas hədəf aldıqları sahələr maliyyə sektoru və nəqliyyat şirkətləridir. Qrup əsasən, uzaqdan qoşulma protokolu (RDP) və ya virtual şəxsi şəbəkə (VPN) zəifliklərindən istifadə edərək hücumlarını həyata keçirmişdir.

Qrupa aid CVE-lər:

CVE-2010-2861, CVE-2018-13379, CVE-2009-3960, CVE-2020-12812, CVE-2019-5591

Qrupun hücum metodologiyası

Qrup ilk növbədə hədəf sistemlərin zəif giriş nöqtələri araşdıraraq, onları zərərli proqramlarla yoluxdurmağa çalışır. Növbəti mərhələdə təhlükəsizlik proqramları deaktiv edilərək, konfidensial məlumatlar əldə olunur.



Qrafik 16. Cring qrupunun yolxuma zənciri

Şəbəkə daxilində hərəkət üçün qrup "Cobalt Strike" proqramından istifadə edir. Bu proqram sistemin müdafiəsini zəiflətmək və "BAT" fayllarını yaymaq üçün istifadə olunur. "BAT" faylları, yükləmə prosesi üçün "Windows CertUtil" proqramından istifadə edərək, təhlükəyə məruz qalmış şəbəkədəki digər sistemlərdə fidyə proqramını yükləmək və icra etmək üçün istifadə olunur. Fidyə proqramı icra edildikdən sonra, şifrələmə rejiminə mane olan xidmətləri və prosesləri deaktiv edir. Bu isə öz növbəsində ehtiyat nüsxə fayllarının silinməsinə, faylların bərpasının çətinləşməsinə səbəb olur.

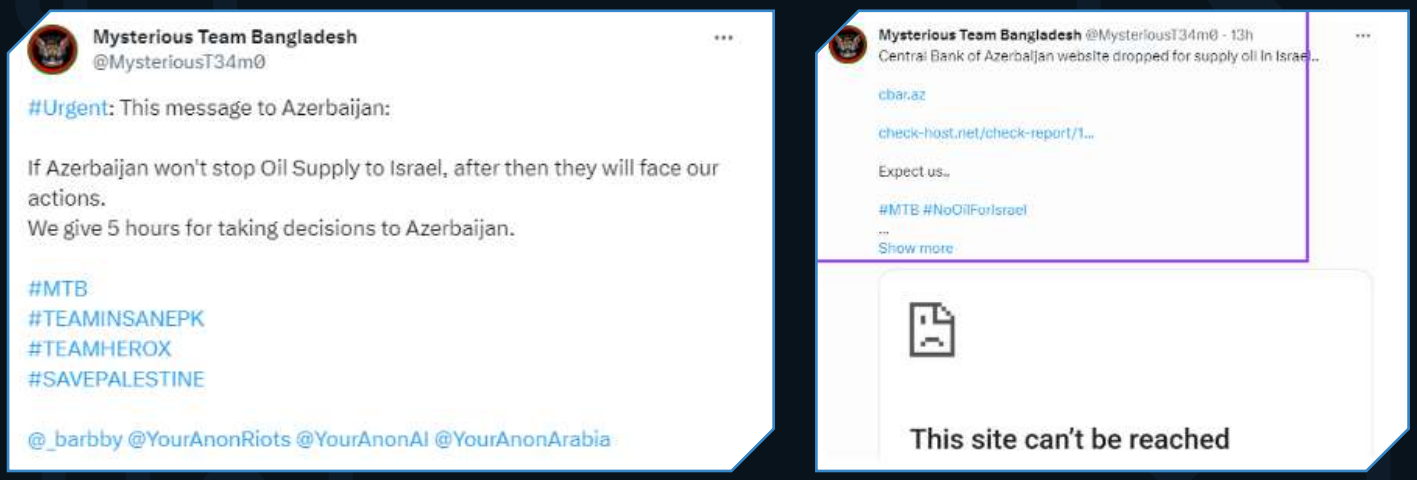
Azərbaycanı hədəf almış

DDoS qrupları

- Mysterious Team Bangladesh
- ANONYMOUS RUSSIA
- Arabian Cyber Team
- Pakistani Leet Hackers
- Carbon
- Anonymous (@Parranttarna)
- Anonymous (@AnonC1B3R)

Mysterious Team Bangladesh

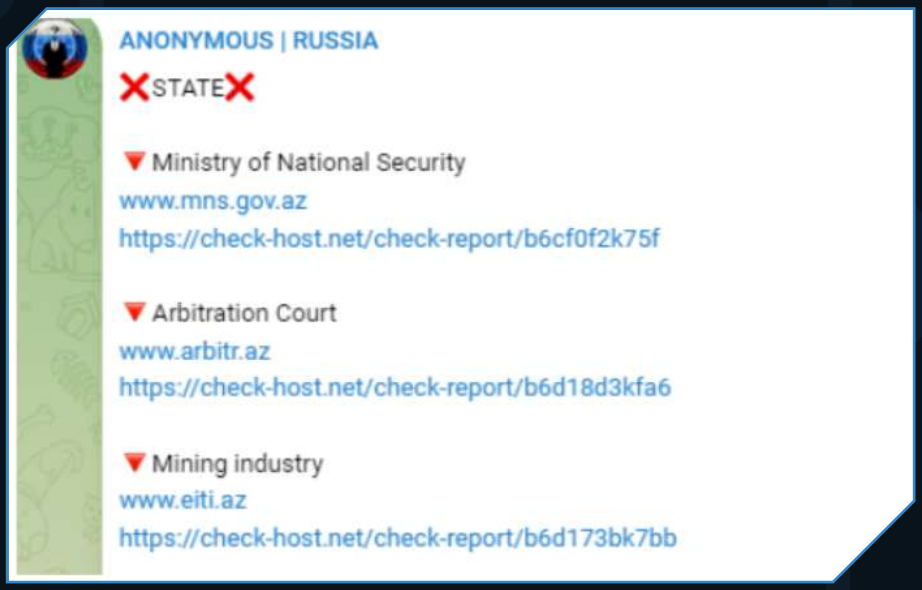
Banqladeş respublikası ilə əlaqəli olduğu ehtimal olunan qrupun əsas hücum hədəfləri başda dövlət orqanları olmaqla , maliyyə xidmətləri, təhsil və səhiyyə qurumlarıdır. "Mysterious Team Banqladesh" qrupu ən çox "DDoS" və uyğunsuz kontent yerləşdirmə hücumları ilə məşğuldur. 2022-ci ilin iyun ayından 2023-cü ilin iyuluna qədər qrup, müxtəlif ölkələrə 770 "DDoS" hücumu və 78 veb-sayta "defecement" hücumu etmişdir.
Qrupun Twitter platformasındakı paylaşımlarında , Azərbaycana qarşı kiber hücumlar həyata keçirdikləri barədə məlumatlar paylaşılmışdır.



Şəkil 7. Mysterious Team Bangladesh qrupunun Twitter paylaşımı

"ANONYMOUS RUSSIA" qrupu

Qrupun Rusiya federasiyası ilə əlaqəli olduğu təxmin edilir. Əsas hücum istiqamətləri başda dövlət orqanları olmaqla , mobil operatorlar və nəqliyyat şirkətləridir. "Anonymous Russia" qrupu ən çox "DDoS" hücumları ilə məşğuldur. "Telegram" platformasındakı paylaşımlarına əsasən, Azərbaycanı hədəfləyən qruplardandır.



Şəkil 8. ANONYMOUS RUSSIA qrupunun Telegram paylaşımı

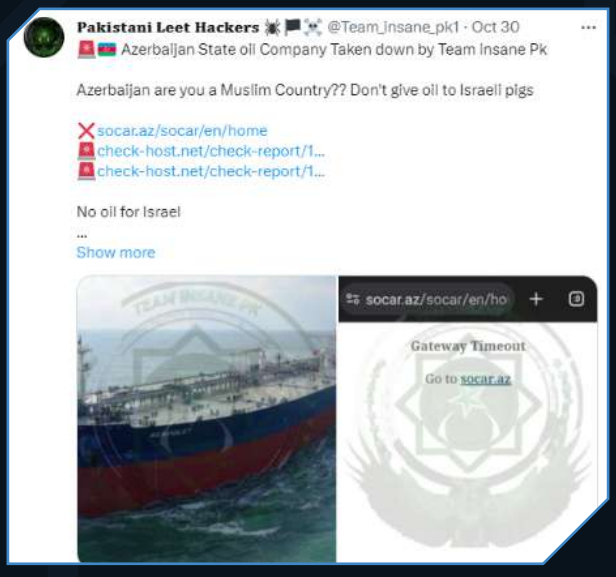
Arabian Cyber Team

Səudiyyə Ərəbistanı əlaqəli olduğu ehtimal olunan qrupun əsas hücum hədəfləri başda dövlət orqanları olmaqla , mobil operatorlar, nəqliyyat və neft şirkətləridir. "Arabian Cyber Team" qrupu ən çox "DDoS" hücumları ilə məşğuldur. "Twitter" platformasındakı paylaşımlarına əsasən, Azərbaycanı hədəfləyən qruplardandır.

Şəkil 9. Arabian Cyber Team qrupunun Twitter paylaşımı

Pakistani Leet Hackers

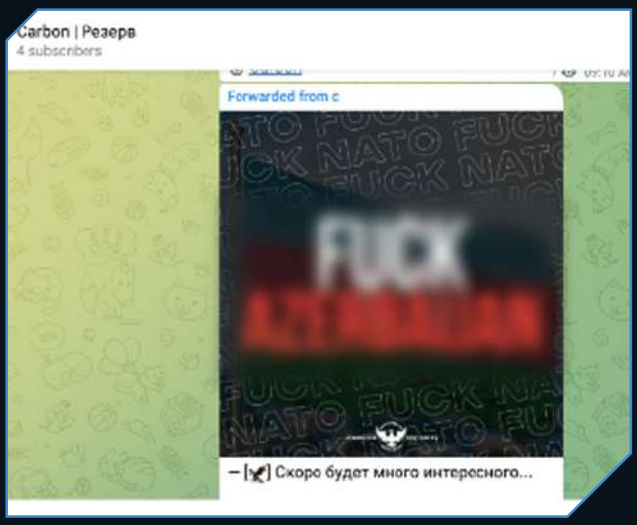
Pakistan respublikası ilə olduğu təxmin edilən qrupun əsas hədəf aldıqları sahələr neft, nəqliyyat şirkətləri, dövlət orqanlarıdır. "Pakistani Leet Hackers" qrupu ən çox DDoS hücumları ilə məşğuldur. "Twitter" platformasındakı paylaşımlarına əsasən, Azərbaycanı hədəfləyən qruplardandır.



Şəkil 10. Pakistani Leet Hackers qrupunun Twitter paylaşımı

Carbon

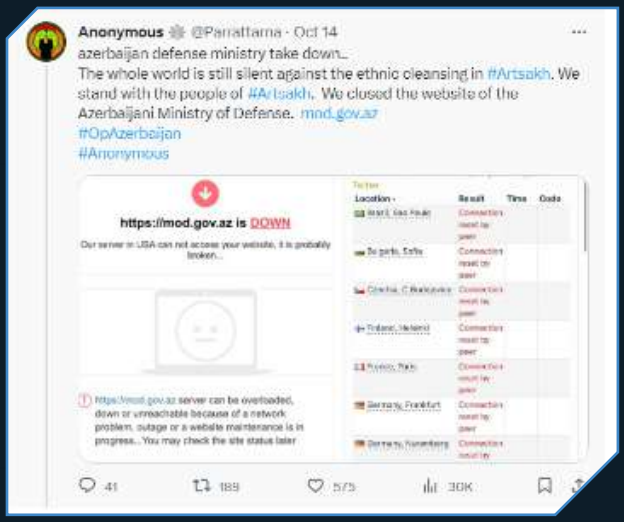
Rusiya federasiyası ilə bağlantılı olduğu ehtimal edilən qrupun əsas hücum hədəfləri dövlət orqanları və banklardır. "Carbon" qrupu daha çox DDoS hücumları ilə məşğuldur. "Telegram" platformasındakı paylaşımlarına əsasən, Azərbaycanı hədəfləyən qruplardandır.



Şəkil 11. Carbon qrupunun Telegram paylaşımı

Anonymous (@Parranttarna)

Qrupun hansı ölkəyə məxsus olduğu bilinmir. Əsas hədəf aldıqları sahələrə bank, telekommunikasiya, xəbər portalları, dövlət orqanları və s. daxildir. "Anonymous" qrupu ən çox DDoS hücumları ilə məşğuldur. "Twitter" platformasındakı paylaşımlarına əsasən, Azərbaycanı hədəfləyən qruplardandır.



Şəkil 11. Anonymous (@Parranttarna) qrupunun Twitter paylaşımı

Anonymous (@AnonC1B3R)

Qrupun hansı ölkəyə məxsus olduğu bilinmir. Əsas hədəf aldıqları sahələrə bank, telekommunikasiya, xəbər portalları, dövlət orqanları və s. daxildir. "Anonymous" qrupu ən çox DDoS hücumları ilə məşğuldur. "Twitter" platformasındakı paylaşımlarına əsasən, Azərbaycanı hədəfləyən qruplardandır.

Şəkil 12. Anonymous (@AnonC1B3R) qrupunun Twitter paylaşımı