
CITIZENSEC
CYBERBRO

Hisobot taqvimi

Umumiy ma’lumotlar

Virus Stealerlar: Turlari, ishlash tartibi va tarqalish usullari

Stealer o’zi nima? Stealer — bu foydalanuvchining shaxsiy ma'lumotlarini (parollar, karta ma'lumotlari, kukilar, kriptovalyuta hamyonlari va boshqalar) o‘g‘irlash uchun mo‘ljallangan zararli dastur.

Stealer Turlari

- Keylogger klaviatura bosishlarini qayd etadi.
- Form Grabber brauzer va ilovalardan ma’lumotlarni o‘g‘irlaydi.
- Clipboard Stealer clipboard (nusxa ko‘chirilgan ma’lumotlar)ni kuzatadi.
- Browser Stealer brauzerdagi login, parollar va kukilarni tortib oladi.
- Cryptocurrency Stealer kriptovalyuta hamyonlaridan ma’lumotlarni o‘g‘irlaydi.
- RAT (Remote Access Trojan) qurilmani masofadan boshqarish imkonini beradi.

Ishlash Tartibi

- Stealer foydalanuvchi tizimiga turli usullar bilan kiradi, jumladan fishing, zararli fayllar yoki eksploitlar orqali.
- Ma’lumotlarni to‘plash bosqichida brauzer, klaviatura, clipboard yoki operativ xotiradan kerakli ma’lumotlar yig‘iladi.
- O‘g‘irlangan ma’lumotlar shifrlanib, yashirin kanallar (Telegram bot, FTP, HTTP, Webhook) orqali hujumchiga yuboriladi.
- Stealer ba’zan iz qoldirmaslik uchun o‘zini avtomatik ravishda o‘chirish funksiyasiga ega bo‘ladi.

Tarqalish Usullari

- Fishing xabarlar (E-mail, Telegram, SMS) orqali zararli fayllarni jo‘natish.
- Crack va aktivator fayllar yordamida foydalanuvchilarning kompyuteriga zararli dasturlarni kiritish.
- Soxta ilovalar va brauzer kengaytmalari orqali zararli kodni ishga tushirish.
- Discord va Telegram kabi messenjerlar orqali zararli fayllarni tarqatish.
- USB orqali avtomatik ishga tushadigan viruslar bilan kompyuterni zararlash.

Himoyalanish Usullari

- Ishonchsiz fayllarni yuklab olmaslik va shubhali havolalarni ochmaslik.
- Rasmiy antivirus dasturlaridan foydalanish va ularni muntazam yangilab borish.

Ikki faktorli autentifikatsiyani yoqish va kuchli parollarni ishlatish.

- Brauzerda saqlangan parollar o‘rniga xavfsiz password manager dasturlaridan foydalanish.
- Windows va boshqa dasturlarni doimiy yangilash orqali eksploitlardan himoyalanish.

LummaC2/Stealer

Stealer is a malware-as-a-service (MaaS)

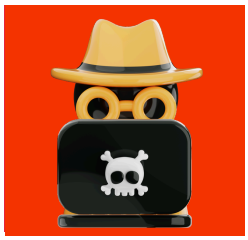
Ma’lumot o’girlovchi ushbu zararli dastur 2022-yildan beri faol ekanligi va internetning kiberjinoyatchilar qatlamida keng tarqalgan hamda xizmat sifatida 250 AQSH narxida obuna sifatida taklif etiladi. 20.000 AQSH dollariga esa uning qisman tuzilish kodlari ham taklif etilgan. LummaC2 dasturi asosan kriptovalyuta hamyonlari, brauzer parollari, shuningdek, boshqa shaxsiy ma’lumotlarni o'g'irlashga mo'ljallangan.

Initial access

Tarqalish va zararlash texnikasi sifatida Lumma turli unikal metodlardan foydalanadi, bular:

- Fishing emaillar
- Turli dastur va brovzerlarning yangilanishlari
- Soxta CAPTCHA orqali
- niqoblangan “double ext” .pdf.ink yoki shunga o’xshash

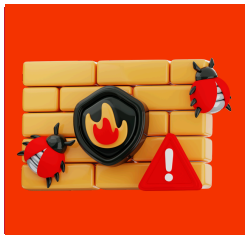
Loader



Lumma o’zi bilan bir qancha zararlovchi boshqa modullarni ham olib kelishi va tizimni zararlashi mumkin, bular :

- ArechClient2/SectopRAT
- Emmenhtal (lolbas orqali zararlash moduli)
- SmartLoader
- HijackLoader/IDAT Loader

Evasion



Lumma AV va xavfsizlik tizimlarini himoyasini aylanib o’tish uchun turli “crypter” lardan foydalanadi, masalan: PureCrypter va CypherIT ushbular zararli dasturni dastlabki tekshiruvlardan qochish orqali ishga tushirishga yordam beradi, shu sabab murakkab bo’lmagan tahdidlarni istalgan kiberjinoyatchi sodir etishi osonlashadi. Lumma odatda to’gridan-to’gri xotiradan ishga tushadi va ma’lumotlarni to’gri C2 serverga uzatadi, so’nggi qadamda dastur o’zini tizimdan o’chirib tashlaydi.

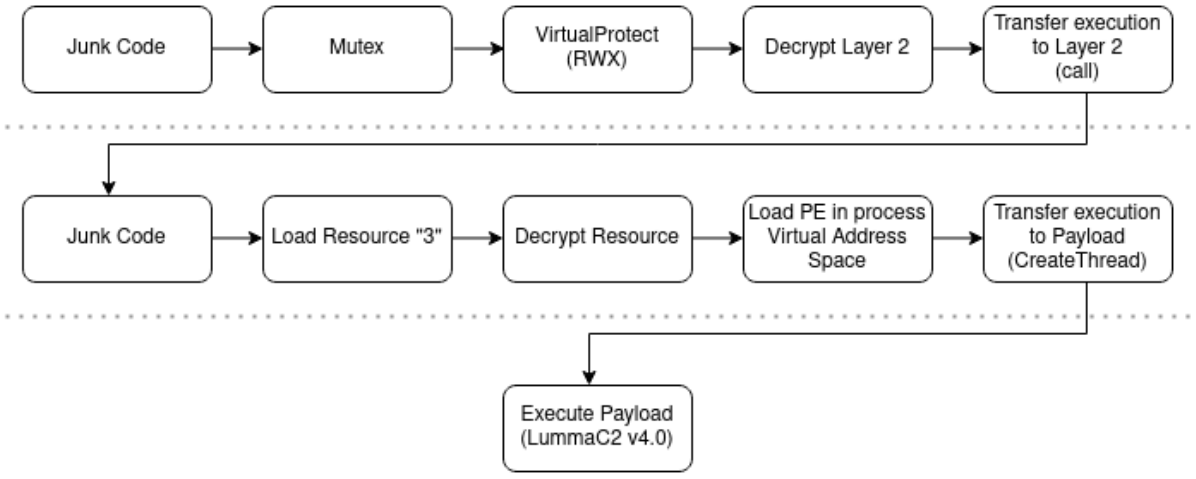
TOP Domenlar	Zararlovchi dastur	Ma’lumotlar soni
[redacted]	LummaC2 Redline Vidar Raccon	• XXXX ortiq foydalanuvchilar haqida
	LummaC2 Redline Vidar Raccon	• XXXX ortiq foydalanuvchilar haqida
	LummaC2 Redline Vidar Raccon	• XXXX ortiq foydalanuvchilar haqida

LummaC2/Stealer

Texnik tahlili

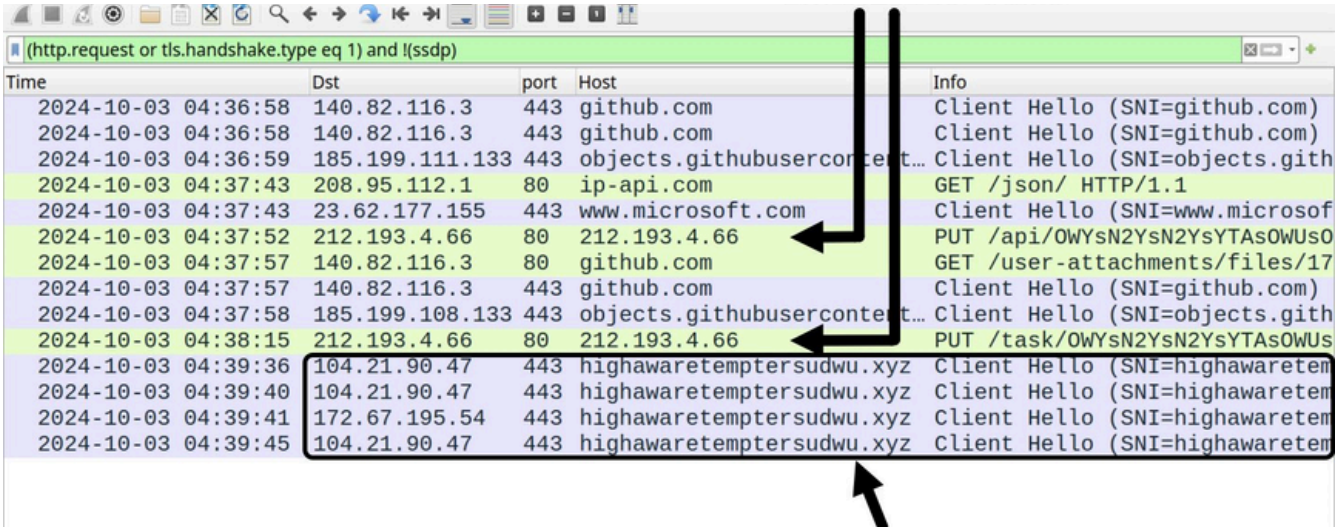
LummaC2 turli obfuscation (chalg'itish) usullari orqali va cryptor, packerlar orqali qayta dekompilyatsiya qilishdan va tuzilish kodlarini o'rganish, hujum qiluvchi server ma'lumotlarini aniqlashni qiyinlashtirishga harakat qiladi. Ushbu zararli dastur turli yangilanishlardan o'tib, hozirda 4.0 versiyasigacha rivojlandi. Ushbu muhim yangilanishlardan ba'zilari quyidagilardir:

- **Control Flow Flattening obfuscation** - obfuskatsiyalash barcha reliz holatlarida amalga oshirildi.
- Yangi **Anti-Sandbox** texnikasi orqali, shaxs sichqonchani harakatlantirmagunicha ishga tushirmaslikni bajaradi, bu orqali virus sandboxda ishlamaydi va aniqlanishni aylanib o'tadi.
- **Stringlar** endi oddiygina o'zgartirilish o'rniga **XOR** orqali shifrlangan.
- Dinamik konfiguratsiya fayllarini **C2** dan olishni qo'llab-quvvatlaydi. Konfiguratsiya **Base64** kodlangan va konfiguratsiya faylning birinchi **32** bayti bilan **XOR** orqali yashirilgan bo'ladi.
- Kiberjinoyatchilar Lumma implant yaratish uchun **crypter** ishlatishga majbur.

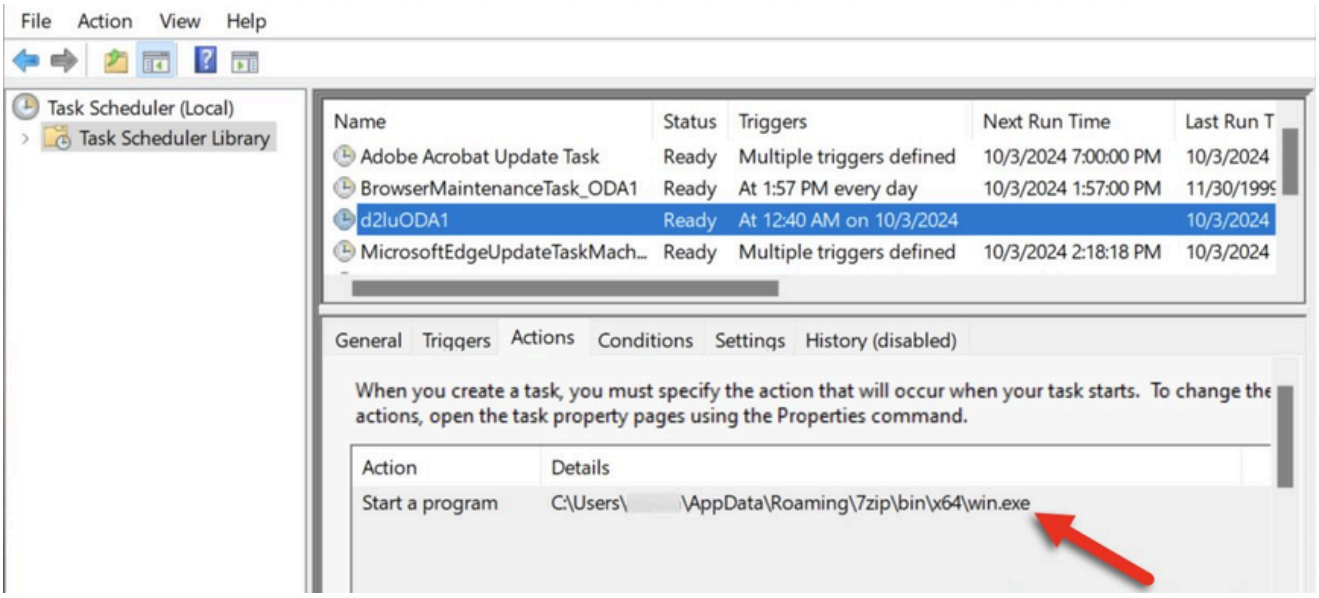


Lumma stealerni aniqlanishdan himoyalovchi packerning asosiy vazifasi, zararli yuklamani obfuskatsiya qilish va uning bajarilishini tizimda qo'shimcha process yaratmasdan ta'minlashdir u bunda "**CreateThread**" dan foydalanadi.

CreateThread — bu Windows operatsion tizimida yangi thread yaratish uchun ishlatiladigan funksiya. U dasturlarda paralel ishni tashkil qilishga yordam beradi. Threadlar bir vaqtning o'zida bir xil dasturda bir necha ishlarni bajarishga imkon beradi, bu esa resurslardan samarali foydalanishni ta'minlaydi va dastur ishini tezlashtiradi.



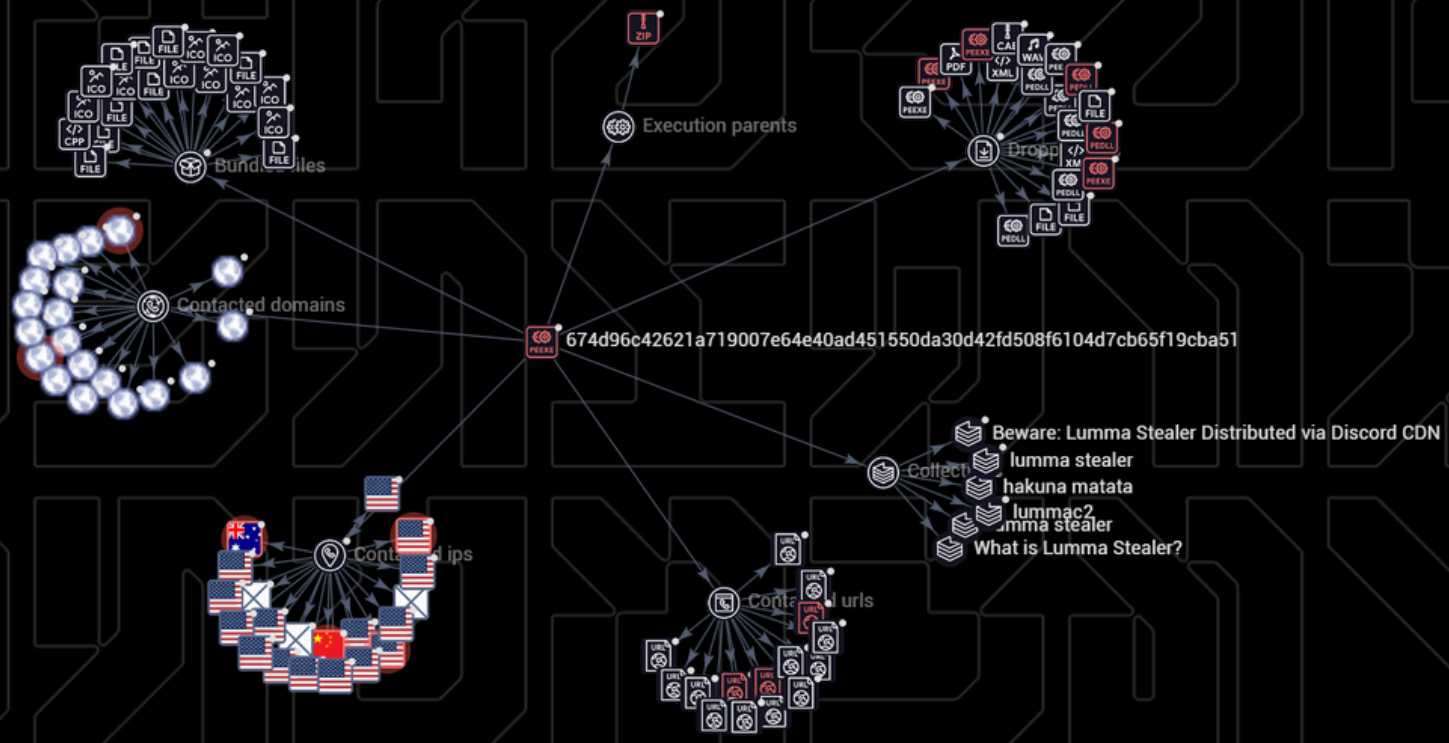
Ushbu rasmda **Lumma SmartLoader** orqali qo'shimcha **RAT** ni ishga tushirmoqda va asosiy stealer traffigini **https** protokoli orqali ximoyalamoqda.



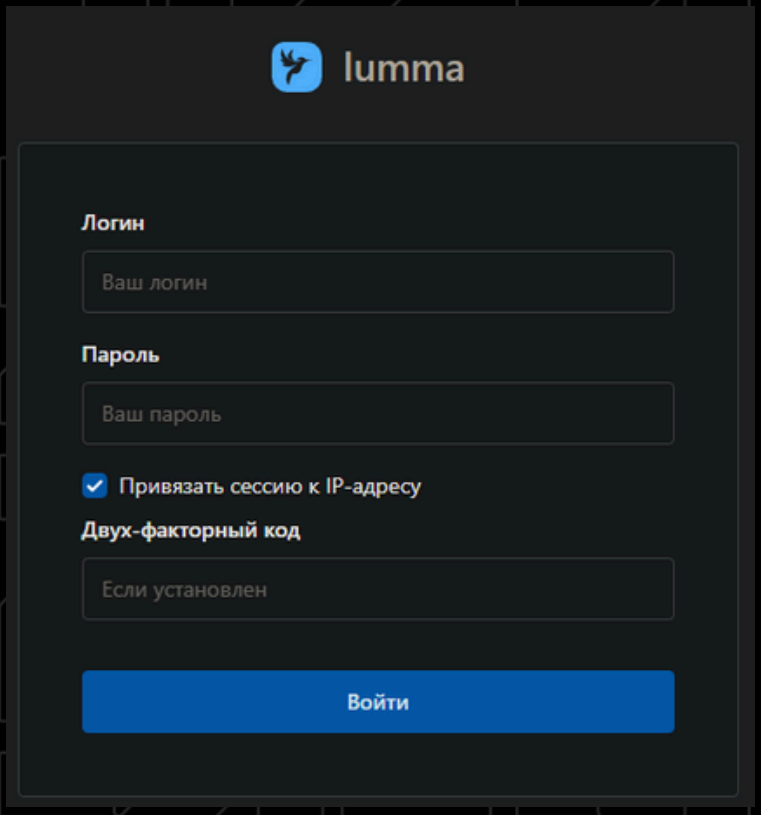
LummaC2 buyerda o'zini doimiy qayta ishga tushirish uchun "**Scheduled task**" ga yozmoqda. Bu tizimda doimiy qolish imkonini beradi.

LummaC2 va Stealer - o’z infratuzilmalarini har bir foydalanuvchi uchun alohida serverlarda tuzib beradi

Bu avvalo asosiy server va jarayonning kiber immunitetini saqlab turadi, kiberjinoyatchi o’z panelini boshqaruvini yo’qotgan taqdirda ham asosiy va boshqa mijozlar xavfsiz qoladi.

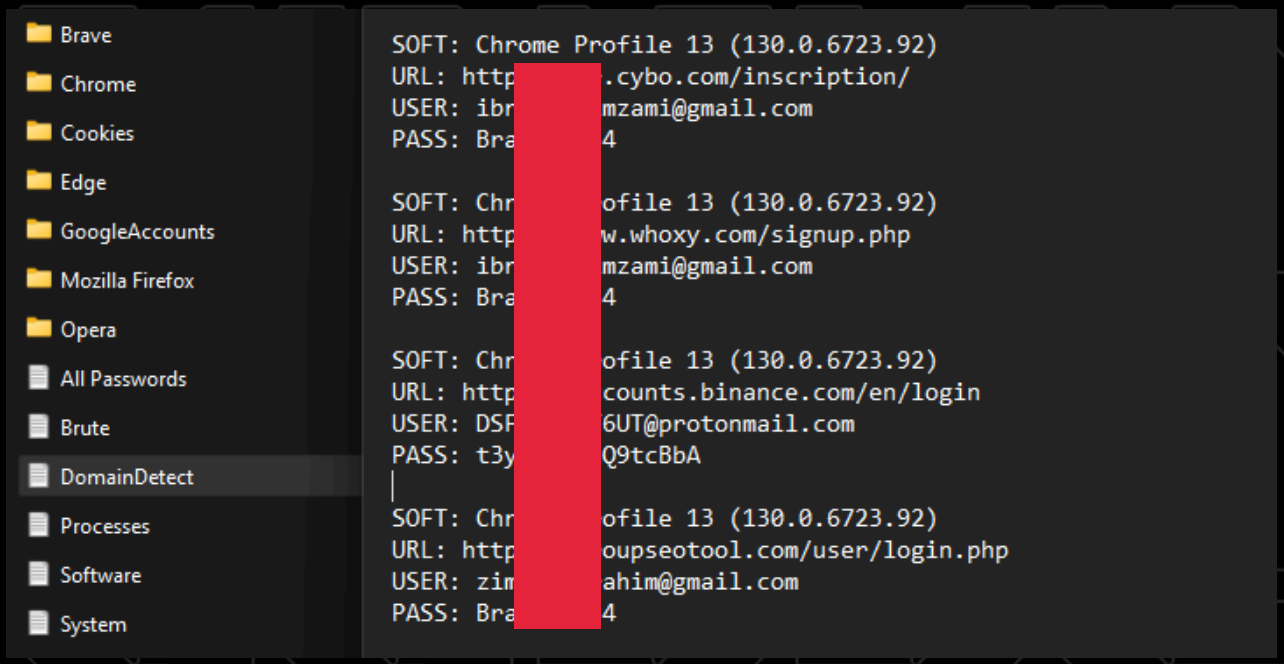


Threat Intelligence orqali Lumma stealeriga tegishli 300ga yaqin serverlar aniqlandi, ularning kirish sahifalarida “**2FA**” orqali tasdiqlash ham joriy qilinganligi, kiberjinoyatchilar o’z mijozlari xavfsizligiga ham e’tibor berishini ko’rsatadi.



LummaC2 zararlagan foydalanuvchilarning nafaqat onlayn hisob raqamlari balki ularning kompyuterlari, qurilmalari ham xavf ostida!

Yuqorida ta’kidlanganidek, Lumma stealeri tizimdagi barcha ma’lumotlarni o’g’irlash bilan birga tizimda boshqa zararli modullarni ham yuklab doimiy kuzatish imkoniyatini qoldirib ketishi mumkin, shu sabab aniqlangan tashkilotlar va ularga tegishli resurslar komplekt kiberxavfsizlik auditidan o’tkazilishi va bunday “backdoor” izlarini o’chirish talab qilinadi.



Lumma qo’lga kiritgan ma’lumotlarni rasmdagi kabi ko’rinishda tartiblab “%APPDATA%\Lumma*” “%LOCALAPPDATA%\Temp*” katalogida vaqtinchalik arxivlaydi va asosiy serverga yuboradi. Ma’lumotlar yuborilgach tizimdan vaqtincha saqlangan arxiv faylni va o’zini ham o’chirib yuboradi. Shu tariqa tizimda faqatgina qo’shimcha zararlash modullaridan boshqa lummaga tegishli hech narsa qolmaydi.

Ma’lumotlaringizni keyingi sahifadagi maxsus bir martalik qrcode orqali yuklab olishingiz mumkin!

Natijalar

CYBER-BRO LLC

CITIZENSEC - CYBER Threat Intelligence hisoboti

Ma’lumotlar qayerdan olinadi ?

CITIZENSEC - CYBER Threat Intelligence

Zamonaviy CTI platformalari, ayniqsa data leak va data breach holatlari bo‘yicha ma’lumotlarni yig‘ishda bir nechta manbalardan foydalanadi. Ushbu hujumlar, ma’lumotlarning ruxsatsiz tarqalishi va tizimlarga noqonuniy kirish bilan bog‘liq bo‘lib, turli tahdid aktorlaridan ehtiyotkorlik bilan yig‘ilgan ma’lumotlar asosida tahlil qilinadi.

Data Leak – bu ma’lumotlarning tasodifiy yoki ehtiyotsizlik sababli ruxsatsiz tarzda tarqalishi yoki oshkor bo‘lishi holati. Bunday vaziyatlarda ma’lumotlar ko‘pincha ochiq internetga yoki noto‘g‘ri odamlarga tushib qoladi. Zamonaviy CTI platformalari data leak holatlariga oid ma’lumotlarni quyidagi manbalardan to‘playdi:

1. **Publicly available forums and temp sites** – ma’lumotlar, masalan, login va parollar, elektron pochta manzillari kabi shaxsiy ma’lumotlar, **Pastebin** yoki boshqa shunga o‘xshash ochiq ammo unikal manzil orqali kirish mumkin bo‘lgan saytlarga joylashtirilishi mumkin.
2. **Dark Web monitoring** – Dark Webda sizib chiqqan ma’lumotlar yoki haqiqiy hisoblarni sotish uchun, ishonchli botlar yoki maxsus tarmoqlar orqali kuzatiladi.
3. **Social Media** – ijtimoiy tarmoqlarda, masalan, Twitter yoki Redditda, foydalanuvchilar tasodifan o‘z ma’lumotlarini oshkor qilishlari mumkin.
4. **Leaked datasets** – ba’zi hollarda, ma’lumotlar to‘plamlari yirik onlayn ma’lumotlar bazalarida yoki o‘zining yuqori xavfsizlikka ega bo‘lmagan joylarda saqlanib qolishi mumkin.

Data Breach – bu ma’lumotlarning tizimga noqonuniy kirish orqali (kiber xujum) o‘g‘irlanishi yoki yo‘qotilishi holatidir. Bunda hujumchilar tizimga kirish uchun turli usullarni ishlatadilar va qo‘lga kiritilgan ma’lumotlar ko‘pincha maxfiy bo‘lgan ma’lumotlar bo‘ladi. Zamonaviy **CTI** platformalari **data breach** holatlarini quyidagi yopiq manbalardan aniqlash va kuzatish uchun ishlatadi:

1. **Commercial Threat Intelligence Feeds** – pullik tahdid ma’lumot oqimlari orqali **data breach** holatlariga oid yangiliklar va **IOC (Indicators of Compromise)** ma’lumotlari olinadi.
2. **Incident Response Reports** – ba’zan kompaniyalar o‘z tizimlariga qilingan hujumlar haqida maxfiy hisobotlar chiqaradilar, bu hisobotlar tahdidlar va ma’lumotlar o‘g‘irlanishi haqida batafsil ma’lumot beradi.
3. **Private Dark Web Intelligence** – xaker guruhlari tomonidan o‘g‘irlangan ma’lumotlar, ba’zan yopiq Dark Web bozorlarida sotiladi. Bu kabi ma’lumotlar ko‘pincha faqat maxsus ruxsatga ega bo‘lgan guruhlar tomonidan aniqlanadi.
4. **Hacker Group Infiltration** – ba'zi hollarda, CTI platformalari ishonchli vositachilar yoki infiltratsiya qilingan kanallar orqali xaker guruhlari vakillari bilan bevosita aloqaga kirishadi. Bunday aloqalar orqali ilgari chiqarilmagan, yopiq ma’lumotlar olingan bo‘lishi mumkin.

xakerlik guruhlari hamda, darknet tarmoqlaridan qo‘lga kiritilgan.

Ximoyalanish choralari

Keyingi qadamlar

Stealer viruslaridan himoyalanish va hujumdan keyingi chora-tadbirlar

1. Brauzer konfiguratsiyasi
   - Brauzerda parollarni saqlashni o‘chirib qo‘yish.
   - chrome://settings/passwords yoki about:preferences#privacy orqali saqlangan ma’lumotlarni tozalash.
   - Brauzerning autofill funksiyasini o‘chirish.
2. OS xavfsizlik sozlamalari
   - AppLocker yoki SRP (Software Restriction Policies) orqali noma’lum dasturlarni bloklash.
   - Windows‘da UAC (User Account Control) ni eng yuqori darajaga o‘rnatish.
   - PowerShell Execution Policy ni Restricted yoki AllSigned rejimiga o‘tkazish.
3. Tarmoq va jarayon monitoringi
   - Windows Defender Firewall yoki IPTables orqali shubhali outbound traffic’ni bloklash.
   - Process Explorer va Sysmon bilan fon jarayonlarini nazorat qilish.
   - Wireshark yoki tcpdump yordamida shubhali tarmoq faolligini tekshirish.
4. Fayl tizimi va reestr himoyasi
   - Windows Group Policy orqali ma’lum direktoriyalarga yozish ruxsatini cheklash.
   - NTFS ACL (Access Control List) sozlamalari bilan foydalanuvchilarni cheklash.
   - Windows Registry Monitoring uchun AuditPol /set /subcategory "Registry" kabi buyruqlar orqali kuzatuvni yoqish.
5. Executable fayllarni nazorat qilish
   - .scr, .js, .vbs, .exe kengaytmali fayllarni avtomatik ishga tushirishni o‘chirish.
   - Autorun o‘chirish: HKLM\Software\Microsoft\Windows\CurrentVersion\Run va Startup kataloglarini tekshirish.
   - Zone.Identifier ni tekshirish: streams.exe -d file.exe bilan internetdan yuklangan fayllarni belgilash.
6. Makrolarni taqiqlash
   - Office makrolari va DDE (Dynamic Data Exchange) ni o‘chirish.
   - gpedit.msc - Microsoft Office Security Settings orqali Disable VBA macros without notification ko‘rinishida sozlash.

Infratuzilmani to’liq auditdan o’tkazishni eng yaxshi va zaruriy yechim sifatida tafsiya qilamiz!

CYBER BRO

Kiberxavfsizlik sohasidagi zamonaviy yechimlarimiz hamda kiber akademiyamiz sizning ushbu sohadagi barcha ehtiyojlaringizga javob bera oladi. Biz bilan bog’laning.

Toshkent shahri, Yunusobod tumani, 12-mavze, 20A-uy

+998 91 791 77 00

info@cyber-bro.uz

CYBER-BRO.uz