Kiberxavfsizlik sohasidagi yangiliklar va innovatsiyalar

Quldoshev Otabek Zarif o’g’li

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari unversiteti Nurafshon filiali

Annotatsiya: Bu maqola kiberxavfsizlik sohasidagi so'nggi yangiliklar va innovatsiyalarni tekshirib chiqish va ularning so'nggi o'zgarishlarni yoritishga bag'ishlangan. Maqola yagona bir xil e'tibor bilan yangi texnologik rivojlanishlarni, kiberxavfsizlikning so'nggi ma'lumotlariga asoslanuvchi innovatsiyalarni va kiber-hujjatlarning eng so'nggi ravishda qanday o'zgarishi mumkinligini baholash uchun amalga oshirilgan.

Kalit so’zlar: Chrome, Vidar, YouTube, Kiberxavfsizlik O'qitish va O'rgatish, Quantum Kiberxavfsizlik, Bulut Xavfsizlik, 5G va IoT Xavfsizlik CoralRaider Xakerlari Ma'lumotlarni O'g'irlashadi, Botlardan foydalanish, AGENT TESLA zararli dasturlari, Targus Buzilgan, Yangi Qakbot DLL, Morphisec Threat Labs, Tahdidlarni Tahlil Qilish, Vedalia APT guruhi, TA547 xakerlari, Midnight, Blizzard Email Hack, Fortinet zaifligi ekspluatatsiya, Zararli Dasturlarga Asoslangan Skanerlash Hujumlaridan Foydalanadigan Xakerlar.

Kiberxavfsizlik sohasidagi yangiliklar va innovatsiyalar hozirda dunyoning har qanday sohasida e'tibor qozonayotgan kritik muammolardan biridir. Bu soha, har kuni yangi xavfsizlik o'rtaligi va kiberatakalar uchun yangi tartibotlarni talab etadi. Quyidagi yo'nalishlar va innovatsiyalar kiberxavfsizlik sohasidagi eng oxirgi yangiliklar hisoblanadi:

Yoshlar uchun Kiberxavfsizlik O'qitish va O'rgatish: Yoshlar kiberxavfsizlik mavzusida o'qitish va o'rgatish jarayonlarida yuqori talabotni o'rganayotganlar. Shunday qilib, oliygohlarda kiberxavfsizlik bo'yicha muhokama darslarini o'tkazish va kiberxavfsizlik texnologiyalarini o'rganish uchun dastlabki harakatlar ko'paymoqda.

Buqalamalar va Xavfsizlikning Avtomatlashtirilishi: Kiberatakalar va kiberxavfsizlik muammo-va-sifatini aniqlash uchun buqalamalar va avtomatlashtirilgan xavfsizlik vositalari keng qamrovda rivojlanmoqda. Bu vositalar, kiberatakalar bilan kurashish va ularga qarshi kurashishning tezligini oshirish uchun zarur bo'lgan turli xil tahlil algoritmlaridan foydalanadi.

Endi-kun: Quantum Kiberxavfsizlik: Kiberxavfsizlik sohasida yangi g'oyalar kvant kompyuterlar va kiberxavfsizlik sohasidagi yangi qirg'ovlar orqali kelajakda kiberxavfsizlikni kuchaytirishga yo'l ochmoqda. Bu texnologiyalar tajribali xakerlarning yaxshiroq bilishlarini ta'minlash uchun muhimdir.

Bulut Xavfsizlik: Bulut xavfsizlik, so'nggi yillarda kiberxavfsizlik sohasida muhim o'rin egallaydi. Bu, ma'lumotlarni bulut tizimlarida saqlashning xavfsizligi va unga kirishni himoya qilish muammolariga yechim topishda katta ahamiyatga ega.

5G va IoT Xavfsizlik: 5G va Internet of Things (IoT) kabi texnologiyalar kiberxavfsizlik sohasida yangi imkoniyatlarni ochadi, lekin birinchi navbatda, ularning xavfsizlik bo'yicha yangi qirg'ovlarni yaratadi. Kiberatakalar, IoT qurilmalari orqali kompaniyalar va shaxslar uchun yangi xavfsizlik muammo-va-sifatlari yaratish imkoniyatiga ega.

CoralRaider Xakerlari Ma'lumotlarni O'g'irlashadi. Xclient stealer va RotBot-bu vetnamlik tahdid aktyori CoralRaider Osiyo va Janubi-Sharqiy Osiyo mamlakatlaridagi qurbonlarning moliyaviy ma'lumotlarini, kirish ma'lumotlarini va ijtimoiy media ma'lumotlarini o'g'irlash uchun foydalanadigan ikkita hujum vositasi. 2023 yildan beri guruh Vetnam lug'atlarini o'zlarining foydali yuklariga bir xil qattiq kodlash sifatida qo'shadigan murakkab yondashuvlar bilan ishlamoqda. Ushbu tahdid guruhining eng so'nggi kompaniyasi Janubiy Koreya, Bangladesh va Xitoy fuqarolariga mo'ljallangan zararli dasturlarni tarqatish uchun oyna yorliq fayllaridan foydalanishni o'z ichiga oladi. Bu mintaqadagi jismoniy shaxslar va korxonalar uchun jiddiy tahdiddir.

Bo'lajak saylovlarga ta'sir qilish uchun AI vositalaridan foydalangan xitoylik xakerlar. Hisobotda xitoylik xakerlar saylovlarga ta'sir qilish uchun Aidan qanday foydalanishlari mumkinligi haqida. Hisobotda hech qanday misol keltirilmagan bo'lsa-da, bu kiber xavfdan ogohlantiradi.

Hatto AI ham deepfake videolarini yaratish, ijtimoiy media saytlarini boshqarish va yuqori darajada rivojlangan kiber huquqbuzarliklarni amalga oshirish uchun ishlatilishi mumkin, bu esa saylovlarga ta'sir o'tkazish uchun juda kuchli vosita hisoblanadi. Bundan tashqari, hisobotda bunday tahdidlarga qarshi kiberxavfsizlik himoyasini kuchaytirish, shu jumladan aniqlash va javob berish imkoniyatlarini yaxshilash ta'kidlangan. Bu, ayniqsa, saylovlar va siyosatga muvofiq, kiber xavflarni o'zgartirish uchun hushyor va faol bo'lish zarurligini ta'kidlaydi. Tahdid Aktyorlari Zararli Dasturlarni YouTube Video Orqali Etkazib Berishadi. Hisobotda Vidar, StealC va Lumma Stealer ma'lumotlarini o'g'irlash zararli dasturlari xakerlar tomonidan YouTube videolari orqali tarqatiladigan so'nggi zararli dastur kompaniyasi ta'kidlangan. Bepul dasturiy ta'minot yoki o'yinlarni yangilash uchun qo'llanma bo'lib ko'rinadigan ushbu videolar buzilgan video o'yinlar va pirat dasturlarga havolalarga ega. Ushbu dasturlar bajarilganda foydalanuvchilarni buzadi. Yosh foydalanuvchilar mashhur kompyuter o'yinlari va YouTube-ning ishonchliligiga ishonadigan ushbu kompaniyani nishonga olishadi. Botlardan foydalanish hisobotda videoning haqiqiyligini oshirish, shuningdek Lumma Stealer-ni discord serverlari orqali o'yin xiylalari niqobi ostida tarqatish usuli deb ham ataladi.

AGENT TESLA zararli dasturlari Chrome va Firefox kirish ma'lumotlarini maqsad qiladi. Agent Tesla zararli dasturi qurbonlarni zararli havolalarni ochish uchun soxta sotib olish buyurtmalariga ega bo'lgan fishing elektron pochta xabarlari yordamida Amerika va Avstraliya tashkilotlariga murojaat qildi. Bosgandan so'ng, Kassandra Protector tomonidan himoyalangan Tesla namunasi yuklab olindi, keyin klaviatura va kirish ma'lumotlarini o'g'irlaydi. Tergov ikkita

aybdorni topdi, asosiy tahdid bo'lgan Bignosa va RDP ulanishlari uchun ko'plab serverlardan foydalangan xudolar va zararli dasturlar kompaniyalari uchun katta elektron pochta ma'lumotlar bazasi. Ushbu kompaniya zararli tarkib bilan spamni tarqatishdan oldin bir necha tayyorgarlik bosqichlarini talab qildi. Bu elektron pochta qo'shimchalari, zararli URL manzillari, hujjatlarga asoslangan tajovuzlar kabi turli xil hujum vektorlaridan foydalanishi mumkin bo'lgan juda moslashuvchan zararli dastur bo'lib, uni tashkilotlar uchun katta xavf tug'diradi. Elektron pochtani kuzatish, blokirovka qilish, o'zgartirish, Fishing, hisobni olish, biznes elektron pochta orqali zararli dastur va to'lov dasturlari kabi tahdidlardan xavfsiz qolish uchun., AI bilan ishlaydigan elektron pochta xavfsizligi echimlarini amalga oshirish tavsiya etiladi.

Targus Buzilgan. Yaqinda Targus kompaniyasi kiberhujum qurboniga aylandi. Bu kiber tahdidlarning boshqa ko'tarilgan holatlari qatoriga kiradi, bu erda o'tgan yilning o'zida xavfsiz elektron pochta shlyuzlari (SEGs) orqali zararli elektron pochta xabarlarining tarqalishi ikki baravar ko'paydi. Shuningdek, sobiq Google muhandisi Linvey Ding tijorat sirlarini o'g'irlash uchun alohida hibsga olingan, xususan sun'iy intellekt (AI). Haqida ma'lumotlar maxfiyligi bundan tashqari, Italiya ma'lumotlarni himoya qilish idorasi (DPA) tergov boshladi OpenAI, yaqinda e'lon qilgan AQSh texnologiya kompaniyasi zamonaviy Ai modeli 'Sora.’ Shunga qaramay, Solarvinds cyberattack, xuddi shu AQSh fikrlash markazini uch marta nishonga olgan va muvaffaqiyatli bo'lgan, tahlilchilar 18000 mijozlari bu hujum bilan siqib chiqarilganiga ishonishadi. Aytishlaricha, bu xizmat ko'rsatish uchun to'lov dasturini ishlab chiqish uchun ushbu sohalardagi mijozlarni moslashtirish orqali amalga oshirilgan. An'anaviy huquqni muhofaza qilish vositalari Adliya vazirligi (DOJ) tomonidan to'lov dasturlari operatorlari va tahdid aktyorlarini yo'q qilish uchun noqonuniy kripto operatsiyalarini nishonga olishda qo'llaniladi.

Yangi Qakbot DLL. 2023 yilda Duck Hunt operatsiyasi paytida tushirilgan Qakbot botneti srtasklardan foydalanadigan o'zgartirilgan DLL bilan qayta paydo bo'ldi.mashinani qayta ishga tushirish paytida uning omon qolishini ta'minlash uchun qat'iylik uchun exe tartibi. Qakbot hali ham fishing kompaniyalari orqali targ'ib qilinadi va ko'pincha mehmondo'stlik sanoatining oz sonli foydalanuvchilarini nishonga olish uchun IRS mavzusidagi elektron pochtadan foydalanadi. Zararli dastur tahlilga qarshi texnikani qo'llaydi, uning tarkibiy qismlarini tomizgich va zararli DLL fayllari yordamida aniqlashdan yashiradi va tizimda davom etishi uchun oyna jarayonlarini boshqaradi.

Morphisec Threat Labs kiber xavfsizlik tahlilchilarining so'nggi topilmalariga ko'ra, xakerlar hozirda png fayllarida Steganografiya zararli dasturlarini yashirish texnikasini amalga oshirmoqdalar. Ushbu usul xavfsizlik tizimlari tomonidan aniqlanishdan qochadi va shu bilan zararli dasturlarni xotirada bajarishga imkon beradi.

Tahdidlarni Tahlil Qilish. Microsoft ikki bosqichli fishing kompaniyasi. Microsoft ikki bosqichli Fishing kompaniyasi LinkedIn foydalanuvchilariga qonuniy OneDrive hujjat havolasi sifatida yashiringan zararli havolali xabarlarni yuborish orqali qaratilgan. Nima hujum ular qurbonlari Microsoft 365 o'g'irlash uchun mo'ljallangan fishing veb-sahifalariga kirib soxta Cloudflare tekshirish xohishi orqali qaratilgan, shunday qilib, u erda zararli o'z ichiga olgan bir so'z hujjatni mavjud OneDrive haqiqiy sahifasiga ularni o'tadi URL bosing qilish va keyin unga yana bir URL embeds deb hisob ma'lumotlari. Ushbu kompaniya LinkedIn kabi ijtimoiy media platformalari o'zlarining foydalanuvchilari haqida fishing uchun ishlatilishi mumkin bo'lgan ochiq ma'lumotlar tufayli tobora zaif tomonlarga aylanib borayotganini ta'kidlaydi. Bu holatda bo'lgani kabi, tahdid aktyorlari TIV bilan hisoblarni buzishga muvaffaq bo'lishdi, chunki ular yaqinda Microsoft 365 fishing kompaniyasida yuzdan ortiq firmalarga ta'sir ko'rsatganidek, multifaktor autentifikatsiyasini (TIV) himoya qilishlari mumkin.

Vedalia APT guruhi katta hajmdagi LNK fayllaridan foydalanadi. Konni yoki "Vedalia APT Group" zararli dastur o'rnatish uchun yangi yo'l bilan keldi, ular operatsiya ularning usullari ba'zi evolyutsiyasi ko'rsatib oversized LNK fayllarni yordamida qilingan. Ushbu usulning maqsadi an'anaviy xavfsizlik choralaridan o'tish va maqsadli tizimlarga ta'sir qilishdir. Ushbu LNK fayllari zararli narsalarni samarali yashiradigan ikkita kengaytmaga ega .lnk kengaytmasi, shuningdek, xavfsizlik dasturlari va tahlilchilar uchun oq bo'shliqlarni haddan tashqari ishlatish orqali ularga o'rnatilgan zararli buyruqlar satrlarini aniqlashni qiyinlashtiradi. LNK fayllarida kuchli buyruq buyruqlarini qidirish va bajarish uchun mo'ljallangan o'rnatilgan buyruq qatori skripti mavjud. Pauershell-ning qonuniy tizim funktsiyalari uning ichida yashirin zararli fayllarni topish, joylashtirish va ochish imkonini beradi. Ushbu kompaniya kiber tahdidlarning o'zgaruvchan manzarasini ta'kidlaydi va tashkilotlar va shaxslar hushyorlikni saqlashlari, xavfsizlik echimlarini yangilashlari va ushbu tahdidlar to'g'risida bilim olishlari kerakligi haqidagi xabarni kuchaytiradi.

TA547 xakerlari AI quvvatli kiber hujumlarni boshladi. Ta547 hacker guruhining RHADAMANTHYS zararli dasturini tarqatadigan AI-quvvatli kiber hujumlari nemis tashkilotlari uchun jiddiy xavf tug'diradi. Ushbu kompaniyalar AI tomonidan yaratilgan kuchli skriptlar va qochish texnikasi kabi ilg'or taktikalardan foydalanadi, potentsial ravishda katta til modellaridan foydalanadi. Tahdid aktyorlari tomonidan murakkab, sun'iy intellektga asoslangan hujum strategiyalarining ushbu evolyutsiyasi bunday murakkab, paydo bo'layotgan tahdidlarga qarshi kurashishga qodir bo'lgan mustahkam, ilg'or elektron pochta xavfsizligi echimlariga shoshilinch ehtiyojni ta'kidlaydi. Midnight Blizzard Email Hack Federal Agentliklari Tahdid. 2024 yil yanvar oyida Microsoft o'zining korporativ elektron pochta tarmog'ida xakerlik bilan shug'ullanganligi ma'lum bo'ldi, bu Rossiya davlat homiyligidagi midnight Blizzard guruhida kuzatilishi mumkin. Guruh faol bo'lmagan test hisob qaydnomasini buzib kirdi va undan Microsoft-ning ba'zi rasmiy elektron pochta manzillariga, shu jumladan yuqori

boshqaruv xodimlariga, shuningdek kiberxavfsizlik, huquq va boshqa sohalardagi hamkasblariga kirish uchun foydalandi. Ular mijozlar tizimiga qo'shimcha kirishga urinish uchun biriktirilgan hujjatlar bilan birga ba'zi elektron pochta xabarlarini olib ketishdi. Xakerlar parolni buzadigan hujumni boshladilar – bu usul bir nechta hisoblarga qarshi bitta parolni sinab ko'rdi-ammo mijozlar ma'lumotlari, ishlab chiqarish tizimlari yoki mulkiy manba kodlariga kirganliklari haqida hech qanday dalil yo'q. Voqea milliy xavfsizlik oqibatlari haqida tashvish uyg'otdi, ayniqsa, federal tashkilotlar shuning CISA bir favqulodda direktifi berish uchun. Microsoft ushbu buzilishlardan ta'sirlangan barcha federal agentliklarni ogohlantirish va o'z tizimlarida xavfsizlikni kuchaytirishga qaratilgan alohida ko'rsatmalarni qo'llash orqali xavfni kamaytirishga harakat qildi. Xakerlar to'xtatilgan domenlarni qurollantiradi. Lotin Amerikasiga qaratilgan davom etayotgan fishing kompaniyasida tahdid qiluvchilar to'xtatilgan domenlarni qurollantirishga murojaat qilishdi. Ular buni “temporary.link” domeni bilan bepul va vaqtinchalik elektron pochta manzillari hamda soxta User-Agent maydonidan foydalangan holda amalga oshirishga muvaffaq bo‘lishdi. Bu shunday elektron xatlarni qabul qiluvchilarni zararli dasturlarni noto'g'ri yuklab olishlari uchun qilingan. Bu potentsial zararli URL manzilni nazarda tutadi, bu jabrlanuvchilarni ikki bosqichli tekshirish jarayoniga yo'naltiradigan, jabrlanuvchining mashinasidan ma'lumot to'plash uchun mo'ljallangan PowerShell skriptini o'z ichiga olgan zararli RAR arxiviga yo'naltiradi.

Fortinet zaifligi ekspluatatsiya qilindi. Fortinet Forticlient EMS zaifligi (CVE-2023-48788) tahdid qiluvchilar ruxsat etilmagan RMM va PowerShell orqa eshiklarini mashinalarga joylashtirish uchun foydalangan xavfsizlik teshigi. Muhim zaiflik Fortinet tomonidan 2024-yilning mart oyida tuzatilgan. Ekspluatatsiya FCMdaemon jarayoniga ulangan tashqi IPdan iborat bo‘lib, bu zararli vositani o‘rnatishga olib keldi. Bu faqat u darhol zaifliklarni tuzatish uchun qanchalik muhim ta'kidlab, orqa eshiklar o'rnatish uchun hujum uchun bir necha

daqiqa davom etdi. Mumkin bo'lgan hujumlarning oldini olish uchun foydalanuvchilar Forticlient EMS-ning joriy versiyalaridan yangilanishi kerak.

Zararli Dasturlarga Asoslangan Skanerlash Hujumlaridan Foydalanadigan Xakerlar. Xakerlar tarmoqlardagi zaifliklarni nishonga olish uchun zararli dasturlarga asoslangan skanerlash hujumlaridan tobora ko'proq foydalanmoqdalar. Qurilmalarni zararli dastur bilan yuqtirish orqali tajovuzkorlar maqsadli tarmoqlarni yashirincha skanerlashi, aniqlashdan qochishi va botnetlarini kengaytirishi mumkin. Ushbu usul tajovuzkorlarga ochiq portlar va dasturiy ta'minotning zaifliklari kabi xavfsizlik kamchiliklarini aniqlashga imkon beradi, bu esa ruxsatsiz kirish va tizimning buzilishini ta'minlaydi. Bu murakkab cyberattacks o'sib borayotgan tahdid ta'kidlab, ommaviy ma'lum oldin so'nggi ko'rish faoliyati, bunday MOVEit zaiflik (CVE-2023-34362) sifatida nishonga zaifliklar, bir hosilasi ko'rsatdi.

Xulosa

Xulosa o’rnida shuni aytish mumkinki. Bu yangiliklar va innovatsiyalar kiber xavfsizlik sohasidagi kritik muammolarga javob berishda katta o'rin egallaydi va kiber xavfsizlikni kuchaytirishga yo'l ochadi. Bu jarayonlar kiber xavflarni oldini oladigan va tizimlarni himoya qiladigan muhim qadriyatga ega.

Foydalanilgan adabiyotlar.

1. https://cybersecuritynews.com/cyber-security-news-weekly-round-up-april/
2. https://gbhackers.com/hackers-deliver-malware-via-youtube-video-game-cracks/

3. https://gbhackers.com/hackers-deliver-malware-via-youtube-video-game-cracks/
4. https://gbhackers.com/agent-tesla-malware-steals-login-credentials-from-chrome-firefox/
5. https://gbhackers.com/targus-hacked/
6. https://cybersecuritynews.com/new-qakbot-dll-windows-persistence/
7. https://cybersecuritynews.com/weaponize-suspended-domains/
8. https://gbhackers.com/microsoft-two-step-phishing-campaign/
9. https://gbhackers.com/vedalia-apt-group-exploits/
10. https://cybersecuritynews.com/malware-driven-scanning-attacks/