TARMOQLARDA RANSOMWARENI OLDINI OLISHDA VEB XAVFSIZLIKNING MUHIMLIGI

[1]Rustamov Alisher Bahodirovich
Muhammad al-Xorazmiy nomidagi TATU Qarshi filiali o'qituvchisi
arustamov_88@mail.ru,
[2]Amirov Akbarshox Dilshod o'g'li
Muhammad al-Xorazmiy nomidagi TATU Qarshi filiali talabasi
amirovakbarshoh05@gmail.com Tel:+998912150812.
https://doi.org/10.5281/zenodo.7493530

Annotatsiya. Ransomware so'nggi yillarda ko'plab tashkilotlar uchun katta muammolar manbai bo'ldi. Ularning ko'pchiligi bu vaziyatdan xabardor bo'lib, o'z kuchlarini ushbu sinf tahdidlaridan himoya qilishga qaratishga harakat qilishadi. Bu ko'pincha ular o'z byudjetlarini veb-xavfsizlikdan uzoqlashtirishini anglatadi. Afsuski, ular uchun bu ularning IT-tizimlarini to'lov dasturidan kamroq xavfsiz qilishlarini anglatadi.

Kalit so'zlar: ransomware, fishing, XSS, SSRF, Cloudflare, WAF.

Hozirda ransomware hujumlari ortib bormoqda. Zararli dasturiy ta'minotning bir turi Ransomware kompyuteringizni garovga olishni o'z ma'lumotlarini shifrlash yoki uni qandaydir tarzda etishmovchiligi bilan ushlab turadi. Ransomware, odatda, jabrlanuvchining kompyuterini ishlashga yaroqsiz holga keltiradigan troyan ot- tipidagi zararli dastur hisoblanadi. Infektsiya ko'pincha huquqni muhofaza qilish idorasidan kelib chiqqan da'vo arizasi bilan bog'liq bo'lib, u jabrlanuvchi kompyuterning mualliflik huquqi bilan himoyalangan materiallar, pirat dasturiy ta'minot va boshqalarni yuklab olish kabi noqonuniy faoliyat bilan shug'ullanganligini bildiradi. Bunga quyidagi sabablarni keltirishimiz mumkin:

Sabab 1. Ransomware hujumning kuchayishi natijasidir

Ransomware bu hujumning o'zi emas, bu haqiqiy hujumning natijasidir.

Agar biz to'lov dasturining ta'sirini kasallik bilan solishtiradigan bo'lsak, ransomware dasturi virus yoki bakteriyalarni ifodalaydi. Virus yoki bakteriyalar uy egasining tanasiga kirgandan so'ng, u ko'payib, butun tizimni yuqtirishga qodir, ko'pincha o'limga olib keladi. Ransomware bilan ham xuddi shunday, u tizimga kirsa, uni to'xtatishning iloji bo'lmasligi mumkin. Biroq, xuddi bakteriya yoki virus o'z-o'zidan bir xostdan ikkinchisiga o'tmagani kabi, to'lov dasturi ham. U qandaydir tarzda tizimga kiritilishi kerak. Va eng samarali himoya choralari bu bosqichda - birinchi navbatda to'lov dasturining tizimga kirishining oldini olishga qaratilgan. Bakteriyalar va viruslar singari, to'lov dasturi ham turli yo'llar bilan yetkazilishi mumkin. Masalan, bakteriya yoki virus teginish yoki tupurik tomchilari orqali tarqalishi mumkin. Xuddi shunday, ransomware

fishing va ijtimoiy muhandislik yoki tizimdagi zaifliklardan foydalanish orqali osonlikcha yetkazib berilishi mumkin. Va bugungi kunda bunday zaifliklarning aksariyati veb-zaifliklardir (sabablarini tushuntirish uchun quyida 3-sababga qarang).

Sabab 2. Veb-hujumlar ransomware tarqatish uchun ishlatiladi

Fishing va ijtimoiy muhandislik ransomware yetkazib berishning eng keng tarqalgan usuli hisoblanadi. Biroq, fishing ko'pincha saytlararo script (XSS) kabi keng tarqalgan veb-zaifliklar tomonidan quvvatlanadi. Bunday zaifliklar tajovuzkorlarga taniqli domen nomlaridan, masalan, sizning kompaniyangiz nomidan, sizning xodimlaringizga va boshqalarga hujumlar yetkazish imkonini beradi. Tasavvur qiling-a, sizning veb-ilovangiz XSS zaifligiga ega. Bu tajovuzkorga xodimlaringizga domen nomingiz bilan URL manzilini yuborish imkonini beradi. Biroq, ushbu domenga tashrif buyurganingizda, xodimingiz avtomatik ravishda zararli yuklab olish joyiga yo'naltiriladi va to'lov dasturini o'rnatuvchini yuklab oladi. Sizningcha, sizning xodimlaringiz bunday nayrangga tushmaydimi? Yana o'ylab ko'ring.

Bundan ham yomoni, tajovuzkor zaif veb-ilovangizdan biznes hamkorlaringizga, mijozlaringizga va hattoki keng jamoatchilikka hujum qilish uchun foydalanishi, tizimingiz zaifligini fosh qilishi va obro'ingizga tuzatib bo'lmas darajada zarar yetkazishi mumkin. Agar buning oldini olishni istasangiz, domen nomlaringizdan foydalanadigan tizimlaringizning hech birida bunday XSS zaifliklari yo'qligiga ishonch hosil qilishingiz kerak.

Sabab 3. Bulutga o'tish ko'proq jinoyatchilarni bulutni maqsad qilganligini anglatadi

1-sababda aytib o'tilganidek, to'lov dasturi maqsadli tizimga turli usullar yordamida, ko'pincha zaifliklardan foydalangan holda yetkazilishi mumkin. Bir muncha vaqt oldin bunday zaifliklarning aksariyati mahalliy tizimlarda mavjud bo'lar edi - bu tarmoq zaifliklari, masalan, eskirgan dasturiy ta'minot yoki mahalliy tarmoqlarning noto'g'ri konfiguratsiyasi natijasida paydo bo'lgan. Endi, so'nggi pandemiyadan keyin ko'plab korxonalar masofaviy ishlashga o'tganda, mahalliy tarmoqlar yanada ko'proq joy yo'qotmoqda.

Bunday mahalliy tarmoqlar bulut bilan almashtiriladi. Va bulut butunlay veb-texnologiyalarga asoslangan. Shu sababli, bulutga o'tish veb zaifliklarining ortib borayotgan ahamiyati bilan bog'liq. Ilgari, ehtimol, faqat marketing veb-saytlariga ta'sir qilgan zaifliklar endi biznes uchun muhim tizimlarga va biznes uchun muhim ma'lumotlarga ta'sir qilishi mumkin.

Ransomware yaratuvchilari ham zamondan oldinda. Ular zararli shifrlovchining mahalliy tarmoq orqali o‘tishi va mahalliy ish stollari va

serverlariga zarar yetkazishi endi yetarli emasligini bilishadi. Ular bilishadiki, bugungi kunda tobora ko'proq potentsial qurbonlar nozik mijozlardan (brauzerlardan) foydalanishadi va bulutda saqlanadigan ma'lumotlarga kirishadi. Shu sababli, ular o'zlarining to'lov dasturlari eng samarali bo'lishini ta'minlash uchun tobora ko'proq veb/bulut zaifliklaridan foydalanishlari kerakligini tushunishadi.

Sabab 4. Tashkilotlar hujum tafsilotlari haqida xabar bermaydilar

O'z biznesingizni to'lov dasturidan qanday himoya qilishni bilish juda qiyin, chunki ransomware qurboni bo'lgan boshqa tashkilotlar ko'pincha o'z tajribalarini baham ko'rmaydilar. Ular shunchaki jamoatchilikka ransomware hujumi qurboni bo'lganliklari haqida xabar berishadi - boshqa hech narsa emas. Bunday xatti-harakat tushunarli. Birinchidan, hujumga uchragan tashkilotlar o'zlarining xavfsizlik kamchiliklarini darhol tuzata olmasligi mumkin. Ikkinchidan, tashkilotlar o'zlarini boshqa hujumlarga ochiqroq qilib qo'ymasliklari uchun hujum vektori tafsilotlarini bo'lishishdan qo'rqishadi. Uchinchidan, ko'pgina tashkilotlar o'z xatolarini tan olish ularning obro'siga putur etkazishi mumkin deb noto'g'ri ishonishadi. Afsuski, bu xatti-harakatlar samarali himoya usullarini ishlab chiqishni sekinlashtiradi va butun dunyo bo'ylab IT xavfsizligiga salbiy ta'sir ko'rsatadi. Bu vaziyatni halokatli virusdan ta'sirlangan va siyosiy sabablarga ko'ra bu haqda hech qanday tafsilotlarni baham ko'rmaydigan mamlakat bilan taqqoslash mumkin.

Sabab 5. Ommaviy axborot vositalari yechimga emas, muammoga e'tibor qaratadi

Vaziyatni yanada yomonlashtiradigan narsa shundaki, hujum tafsilotlari ma'lum bo'lgan kamdan-kam hollarda, aksariyat ommaviy axborot vositalari bunday tafsilotlarni eslatmaslikka qaror qilishadi. Bu barcha xavfsizlik buzilishi holatlarida to'g'ri. Buning o'rniga, ommaviy axborot vositalari ransomware hujumining biznesga ta'siri kabi mashhur mavzularga e'tibor qaratadi. Masalan, 2019 yildagi Capital One ma'lumotlarining buzilishi server tomonidagi so’rovlarni qalbakillashtirish (SSRF) tufayli sodir bo'lganligini bilish uchun siz qidiruv tizimlarini chuqur o'rganishingiz kerak bo'ladi. Aksariyat ommaviy axborot vositalari bu muhim ma'lumotni eslatib o'tishga shoshilmadi.

Ommaviy axborot vositalari va biznes xulq-atvori nuqtai nazaridan, ransomware hamma joyda biznes uchun yanada ko'proq muammo bo'lishiga olib keladi, eng yaxshi amaliyotlarga amal qiladigan yirik korxonalar mavjudligini ko'rish yoqimli ajablantiradi. Buning Cloudflare-dan yaxshiroq namunasi yo'q. Misol uchun, 2019-yilda Cloudflare inson xatosi va veb-ilovalar xavfsizlik devori (WAF) dan foydalanish natijasida katta uzilishni boshdan

kechirganida , ular butun voqeani ta'sirchan darajada tafsilotlardan foydalangan holda tasvirlab berishdi - bu ularning odatiy amaliyoti.

Xulosa qilib aytganda OAVga hujumning ma'lum tafsilotlarini baham ko'rishni chin dildan tavsiya qilamiz. Agar biz ma'lumotni baham ko'rsak va ransomware hujumining birinchi qadamlari haqida bilib olsak, kelajakda bunday hujumlardan o'zimizni himoya qilish uchun barchamiz yaxshi imkoniyatga ega bo'lamiz.

Foydalanilgan adabiyotlar:

1. Шубинский И.Б. Структурная надёжность информационных систем. Методы анализа /Ульяновск: Печатный двор, 2012.
2. ISO 31000:2009. Risk management — Principles and guidelines.
3. IEC/ISO 31010:2009. Risk management — Risk assessment techniques.
4. ISO 15190:2003. Medical laboratories — Requirements for safety.
5. BS 31100:2008. Risk management — Code of practice.