मैलवेयर हमला के प्रकार

मैक्रो वायरस

ये वायरस माइक्रोसॉफ्ट वर्ड या एक्सेल जैसे एप्लिकेशन को संक्रमित करते हैं। मैक्रो वायरस एक एप्लिकेशन के आरंभीकरण अनुक्रम से जुड़ते हैं। जब एप्लिकेशन खोला जाता है, तो वायरस एप्लिकेशन पर नियंत्रण स्थानांतरित करने से पहले निर्देशों को निष्पादित करता है। वायरस खुद को दोहराता है और कंप्यूटर सिस्टम में अन्य कोड के साथ संलग्न करता है।[1]

फाइल इंफ़ेक्टर्स

फ़ाइल इंफ़ेक्टर वायरस आमतौर पर खुद को निष्पादन योग्य कोड में संलग्न करते हैं, जैसे .इएक्सइ फ़ाइलें। कोड लोड होने पर वायरस इंस्टॉल हो जाता है। एक फ़ाइल इन्फ़ेक्टर का दूसरा संस्करण एक ही नाम के साथ एक वायरस फ़ाइल बनाकर एक फ़ाइल के साथ जुड़ता है,लेकिन -.इएक्सइ एक्सटेंशन में। इसलिए जब फ़ाइल खोली जाती है, तो वायरस कोड निष्पादित होगा।[2]

सिस्टम या बूट-रिकॉर्ड इन्फ़ेक्टर

एक बूट-रिकॉर्ड वायरस हार्ड डिस्क पर मास्टर बूट रिकॉर्ड से जुड़ता है। जब सिस्टम शुरू किया जाता है, तो यह बूट सेक्टर को देखेगा और वायरस को मेमोरी में लोड करेगा, जहां यह अन्य डिस्क और कंप्यूटर में प्रचारित कर सकता है।[3]

पॉलीमोरफिक वायरस

ये वायरस अलग-अलग एन्क्रिप्शन और डिक्रिप्शन की चक्रों के माध्यम से खुद को छुपाते हैं। एन्क्रिप्टेड वायरस और एक संबद्ध म्यूटेशन इंजन शुरू में डिक्रिप्शन प्रोग्राम द्वारा डिक्रिप्ट किए जाते हैं। वायरस कोड के एक क्षेत्र को संक्रमित करता है।

म्यूटेशन इंजन फिर एक नई डिक्रिप्शन रूटीन विकसित करता है और वायरस म्यूटेशन इंजन और वायरस की कॉपी को एल्गोरिथम के साथ एन्क्रिप्ट करता है नई डिक्रिप्शन रूटीन के अनुरूप। म्यूटेशन इंजन और वायरस का एन्क्रिप्टेड पैकेज नए कोड से जुड़ता है और प्रक्रिया दोहराई जाती है। ऐसे वायरस का पता लगाना मुश्किल होता है, लेकिन उनके स्रोत कोड के कई संशोधनों के कारण उच्च स्तर की एन्ट्रॉपी होती है। एंटी-वायरस सॉफ्टवेयर या प्रोसेस हैकर जैसे फ्री टूल्स इस फीचर का इस्तेमाल कर उनका पता लगा सकते हैं।[4]

स्टेल्थ वायरस

स्टेल्थ वायरस खुद को छुपाने के लिए सिस्टम फंक्शन का सहारा लेते हैं। वे मालवेयर डिटेक्शन सॉफ्टवेयर से समझौता करके ऐसा करते हैं ताकि सॉफ्टवेयर एक संक्रमित क्षेत्र को असंक्रमित होने की सूचना देगा। ये वायरस किसी संक्रमित फ़ाइल के आकार में किसी भी वृद्धि या फ़ाइल के अंतिम संशोधन के समय और तारीख में परिवर्तन को छिपाते हैं।[5]

लॉजिक बॉम्ब

लॉजिक बम एक सॉफ़्टवेयर सिस्टम में जानबूझकर डाला गया कोड का एक टुकड़ा है जो निर्दिष्ट शर्तों के पूरा होने पर एक दुर्भावनापूर्ण फ़ंक्शन को शुरू कर देगा। उदाहरण के लिए, एक प्रोग्रामर कोड का एक टुकड़ा छिपा सकता है जो वेतन डेटाबेस ट्रिगर जैसी फ़ाइलों को हटाना शुरू करता है।[6]

ड्रॉपर

एक ड्रॉपर एक प्रोग्राम है जिसका उपयोग कंप्यूटर पर वायरस को स्थापित करने के लिए किया जाता है। कई उदाहरण मे, ड्रॉपर दुर्भावनापूर्ण कोड से संक्रमित नहीं है और इसलिए वायरस-स्कैनिंग सॉफ़्टवेयर द्वारा इसका पता नहीं लगाया जा सकता है। एक ड्रॉपर इंटरनेट से कनेक्ट हो सकता है और वायरस सॉफ़्टवेयर के लिए अपडेट डाउनलोड कर सकता है जो एक समझौता प्रणाली में निवासी है।[7]

रैंसमवेयर

रैंसमवेयर एक प्रकार का मैलवेयर है जो पीड़ित व्यक्ति की पहुंच को अवरुद्ध करता है जब तक फिरौती का भुगतान नहीं किया जाता है, तब तक डेटा और इसे प्रकाशित या हटाने की धमकी देता है। जबकि कुछ सरल कंप्यूटर रैंसमवेयर सिस्टम को इस तरह से लॉक कर सकते हैं जो किसी जानकार व्यक्ति को उल्टा करना मुश्किल नहीं है। अधिक उन्नत मैलवेयर 'क्रिप्टो वायरल एक्सटॉर्शन' नामक तकनीक का उपयोग करता है, जो पीड़ितों की फ़ाइलों को इस तरह से एन्क्रिप्ट करता है जिससे डिक्रिप्शन कुंजी के बिना उन्हें पुनर्प्राप्त करना लगभग असंभव हो जाता है।[8]

एडवेयर

एडवेयर एक सॉफ्टवेयर एप्लीकेशन है जिसका इस्तेमाल कंपनियां मार्केटिंग के लिए करती हैं/किसी भी कार्यक्रम के चलने के दौरान विज्ञापन बैनर प्रदर्शित किए जाते हैं। किसी भी वेबसाइट को ब्राउज़ करते समय एडवेयर आपके सिस्टम में स्वचालित रूप से डाउनलोड किया जा सकता है और इसे पॉप-अप विंडो के माध्यम से या कंप्यूटर स्क्रीन पर स्वचालित रूप से दिखाई देने वाले बार के माध्यम से देखा जा सकता है।[9]

स्पाइवेयर

स्पायवेयर एक प्रकार का प्रोग्राम है जो उपयोगकर्ताओं, उनके कंप्यूटर या उनकी ब्राउज़िंग आदतों के बारे में जानकारी एकत्र करने के लिए स्थापित किया जाता है। यह आपके ज्ञान के बिना आपके द्वारा किए गए सभी चीजों को ट्रैक करता है और डेटा को दूरस्थ उपयोगकर्ता को भेजता है। यह इंटरनेट से अन्य दुर्भावनापूर्ण प्रोग्रामों को डाउनलोड और इंस्टॉल कर सकता है। स्पाइवेयर एडवेयर की तरह काम करता है लेकिन आमतौर पर एक अलग प्रोग्राम है जो अनजाने में स्थापित होता है जब आप एक और फ्रीवेयर एप्लिकेशन इंस्टॉल करते हैं।[10]

संदर्भ

1. *"What is macro virus? - Definition from WhatIs.com" (https://searchsecurity.techtarget.com/definition/macro-virus)* . *SearchSecurity (अंग्रेज़ी में). अभिगमन तिथि 2020-08-23.*
2. *"File Infecting Viruses - Definition - Trend Micro USA" (https://www.trendmicro.com/vinfo/us/security/definition/file-infecting-viruses)* . *www.trendmicro.com. अभिगमन तिथि 2020-08-23.*
3. *"What is a Boot Sector Virus?" (https://usa.kaspersky.com/resource-center/definitions/boot-sector-virus)* . *usa.kaspersky.com (अंग्रेज़ी में). 2017-12-07. अभिगमन तिथि 2020-08-23.*
4. *"Polymorphic virus - Definition - Trend Micro USA" (https://www.trendmicro.com/vinfo/us/security/definition/Polymorphic-virus)* . *www.trendmicro.com. अभिगमन तिथि 2020-08-23.*
5. *"What is a Stealth Virus?" (https://www.kaspersky.co.in/resource-center/definitions/stealth-virus)* . *www.kaspersky.co.in (अंग्रेज़ी में). 2017-08-31. अभिगमन तिथि 2020-08-23.*
6. *"What is a Logic Bomb? - Definition from WhatIs.com" (https://searchsecurity.techtarget.com/definition/logic-bomb)* . *SearchSecurity (अंग्रेज़ी में). अभिगमन तिथि 2020-08-23.*
7. *"Dropper" (https://encyclopedia.kaspersky.com/glossary/dropper/)* . *encyclopedia.kaspersky.com (अंग्रेज़ी में). अभिगमन तिथि 2020-08-23.*
8. *Fruhlinger, Josh (2020-06-19). "Ransomware explained: How it works and how to remove it" (https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html)* . *CSO Online (अंग्रेज़ी में). अभिगमन तिथि 2020-08-23.*

9. *"Adware - What Is It & How To Remove It" (https://www.malwarebytes.com/adware/)* . *Malwarebytes (अंग्रेज़ी में)*. *अभिगमन तिथि 2020-08-23.*
10. *"What is spyware? And how to remove it" (https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html)* . *us.norton.com (अंग्रेज़ी में)*. *अभिगमन तिथि 2020-08-23.*

Last edited 2 years ago by AmitJ 2019201037