بسمه‌تعالی

گزارش فنی بدافزار Nivdort

۱ معرفی بدافزار

Nivdort بدافزاری است که عمدتاً برای سرقت اطلاعات حساب‌های کاربری قربانیان به ویژه اطلاعات حساب‌های بانکی آن‌ها به کار می‌رود. مهمترین راه‌کار انتشار این بدافزار از طریق هرزنامه‌هاست، لیکن انتشار این بدافزار از طریق شبکه‌های اجتماعی مانند فیس‌بوک نیز گزارش شده است. این بدافزار پس از اجرا بر روی سیستم قربانی، با افزودن کلیدهای خاصی به رجیستری ویندوز سبب اجرای مجدد خود پس از هربار راه‌اندازی مجدد ویندوز می‌گردد. میزان انتشار این بدافزار در دنیا قابل قیاس با سایر بدافزارهای مشهور بانکی مانند Zeus نیست.

۲ شناسایی سیستم آلوده از طریق لاگ‌های شبکه

تمامی میزبان‌هایی که نام دامنه‌هایی را Resolve کرده باشند که در آن‌ها ترکیبی از کلمات زیر به کار رفته باشد، ممکن است آلوده باشند و بایستی مورد بررسی قرار گیرند:

journey, destroy, against, night, within, effort, street, better, husband, little, doubt, decide, suffer, through, trade, gather, ridden, chair, large, record, forget, would, flier, quiet, belong, those, captain, electric, increase, remember, bread, season, degree, answer, think, chief, order, leader, rather, strange, forward, glass, present, college, require, heaven, morning, history, difficult, pleasant, often, middle, heavy, various, amount, thick, heard, necessary, alone, twelve, gentle, return, weather, class, movement, building, fresh, gentleman, fellow, broken, summer, thought, outside, evening, experience, already, double, result, crowd, water, store, doctor, follow, begin, prepare, strength, woman, party, might, pretty, member, known, desire, still, smoke, fight, expect, person, severa, simple, figure, picture, winter, finish, because, machine, laugh, mother, though, cigarette, subject, leave, sudden, whether, mountain, perhaps, children, either, sweet, several, foreign, right, possible, window, family, english, probably, material, shore, welcome, dollar, proud, should, industry, opinion, contain, character, nature, board, enough, supply, settle, office, device, beyond, silver, forever, valley, matter, school, together, question, flower, bring, special, demand, father, hunger, built, storm, written, around, realize, complete, short, became, promise, basket, ladder, needle, enter, govern, distance, language, arrive, before, being, sister, bottom, labor, spent, while, control, therefore, minute, listen, corner, shout, apple, training, carry, thrown, length, laughter, indeed, consider, almost, attempt, orderly, neighbor, clear, smell, include, safety, chance, market, twenty, beauty, clean, ready, course, people, understand, succeed, behind, produce, stream, nation, bottle, please, dried, round, angry, likely, notice, fancy, during, friend, reason, square, value, spread, general, early, north, future, meeting, report, understood, garden, paint, brown, women, daughter, broad, between, butter, student, nothing, soldier, divide, condition, fifteen, glossary, article, worth, except, further, bicycle, become, strong, found, president, success, wagon, until,

kitchen, shoulder, continue, airplane, wonder, guard, advance, station, goodbye, object, measure, choose, afraid, period, escape, space, problem, yellow, wheat, single, always, difference, bridge, cover, whose, company, trouble, spring, caught, banker, without, above, probable, finger, master, straight, discover, fence, stranger, third, fortieth, childhood, dinner, although, circle, however, animal, travel, modern, close, anger, charge, forest, every, branch, separate, receive, clothes, borrow, toward, electricity, million, honor, catch, system, public, number, heart, strike, mayor, manner, century, business, power, mister, method, service, direct, instead, surprise, bright, letter, nearly, speak, shake, write, believe, health, quarter, distant, train, pleasure, delight, white, neither, eearly, trust, dress, position, perfect, partial, battle, ano, fam, us, appear, country, suppose, action, river, brought, explain, beside, inside, different, happen, niece, share, oclock

به عنوان مثال، برخی از نام‌های دامنه این‌چنینی عبارتند از:

- Familysmell.net
- Childrennearly.net
- Familyearly.net

۳ بررسی وجود آلودگی

نشانه‌های وجود آلودگی به بدافزار Nivdort بر روی سیستم عبارتند از:

۱. وجود یکی از کلیدهای زیر در رجیستری ویندوز:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Font TCP/IP Adapter Key Encryption
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Font TCP/IP Adapter Key Encryption

۲. وجود فایل و پوشه‌ای مشابه با آنچه در ذیل ارایه شده است بر روی سیستم:

- C:\hcjqpqng\w9fax19j9vwxgicy9tg.exe

۳. وجود پروسه‌ای با نام ximefm... بر روی سیستم

۴ نحوه پاک‌سازی سیستم

فرآیند پاک‌سازی سیستم از بدافزار Nivdort بدین صورت است:

۱. بایستی ابتدا اجرای پروسه‌ی ximefm... و تمامی پروسه‌های زیر مجموعه آن متوقف شوند.

۲. سپس بایستی پوشه‌ی C:\hcjqpqng و تمامی محتویات آن از روی سیستم حذف شوند.

۳. در مرحله سوم بایستی کلیدهای ذکر شده در بند ۱ قسمت قبل از روی سیستم حذف شوند.

۴. بایستی در گام آخر سیستم را مجدداً راه‌اندازی نمود.

۵ بررسی پاک بودن سیستم

به منظور حصول اطمینان از پاک بودن سیستم لازم است:

۱. پروسه‌ای با نام تصادفی (ximefm...) بر روی سیستم در حال اجرا نباشد.

۲. پوشه‌ای با نام تصادفی بر روی درایو C (C:\hcjqpqng) بر روی سیستم وجود نداشته باشد.

۳. کلیدهای ذکر شده در رجیستری ویندوز وجود نداشته باشند.

۴. سیستم قصد برقراری ارتباط با نام‌های دامنه‌ای که قبلاً ذکر گردید را نداشته باشد.

۶ توصیه‌های امنیتی برای پیشگیری

- خودداری از باز نمودن ایمیل‌های ناشناس
- خودداری از اجرای فایل‌های اجرایی ناشناس به خصوص فایل‌های دریافتی از طریق ایمیل
- به روز رسانی نرم‌افزار ضد بدافزار