حملات ماحیگیری هم‌نگاره

و چالش نام‌های دامنه اینترنتی بین‌المللی

گروه تحلیل تهدید
شرکت رامونا پردازش نگار

< فهرست مطالب >

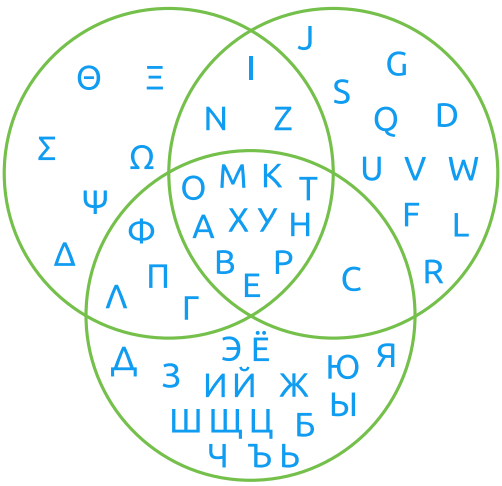
>_ وقتی به چشم‌ها هم نمی‌شود اعتماد کرد!

«ماهیگیری[1] هم‌نگاره» یا Homograph Phishing - که با نام Homoglyph Phishing نیز شناخته می‌شود - تکنیکی است که در آن از نویسه(های) مشابه با نویسه(های) یک سایت واقعی به‌منظور جعل[2] نشانی سایت و در نتیجه قابل باور ساختن آن از دید کاربر استفاده می‌شود.

استفاده از 0 (عدد صفر) بجای o در g00gle.com، l (حرف i بزرگ) در paypal.com و rn (ترکیب حروف r و n) بجای m در rnicrosoft.com نمونه‌هایی از بکارگیری این روش با هدف جعل دامنه‌های معروفی همچون google.com paypal.com و microsoft.com هستند. هر چند در نگاه اول، این تکنیک ساده به نظر می‌رسد اما یکی از شگردهای موفق مهاجمان و گردانندگان حملات ماهیگیری است که همچنان بسیاری از کاربران به دام آن می‌افتند.

اما ماهیگیری هم‌نگاره، همیشه این‌قدر ابتدایی نیست. در نمونه‌های پیچیده‌تر مهاجم از ثبت دامنه اینترنتی بین‌المللی بهره می‌گیرد. از بیش از یک دهه قبل امکان ثبت دامنه‌های اینترنتی به زبان‌های غیرلاتین از طریق کدگذاری یونی‌کد[3] فراهم شده است. یک دامنه ثبت شده به زبانی غیرلاتین، به عنوان یک «نام دامنه بین‌المللی» یا Internationalized Domain Name - به اختصار IDN - شناخته می‌شود.

حمله هم‌نگاره از طریق ثبت یک دامنه اینترنتی بین‌المللی یا IDN Homograph Attack تکنیکی است که در جریان آن مهاجم از شباهت ظاهری و همسانی حروف در زبان‌های مختلف برای فریب کاربر سوءاستفاده می‌کند. به عبارت دیگر، مهاجم با استفاده از حروفی هم‌شکل اما با زبانی متفاوت اقدام به ثبت دامنه‌ای مشابه با یک دامنه معروف می‌کند. به‌خصوص آن‌که در الفبای لاتین، یونانی و سیریلیک حروف هم‌نگاره متعددی به چشم می‌خورد. برای مثال، نویسه O، پانزدهمین حرف الفبای یونانی، Ο، پانزدهمین حرف الفبای لاتین و O یکی از حروف الفبای سیریلیک است که همگی در قالب یونی‌کد به نحوی هم‌نگاره ظاهر می‌شوند.



شکل ۱ حروف هم‌نگاره در الفبای لاتین، یونانی و سیریلیک

[1] Phishing // استفاده از حرف «ح» بجای «هـ» در کلمه «ماهیگیری» نیز از جایگزینی «f» با «ph» در «fishing» الگوبرداری شده است.
[2] Spoofing
[3] Unicode

در حمله‌ای فرضی، کاربر rpnegar.com ممکن است متقاعد به کلیک بر روی لینک دامنه جعلی rpnegar.com شود که در آن حرف لاتین a با حرف سیریلیک a جایگزین شده و پیش‌تر توسط مهاجم ثبت گردیده است (جدول ۱)؛ حروفی که در بسیاری از فونت‌ها کاملا هم‌نگاره هستند (جدول ۲).

rpnegar.com (واقعی)			rpnegar.com (جعلی)		
نویسه	عنوان یونی‌کد	شناسه یونی‌کد	نویسه	عنوان یونی‌کد	شناسه یونی‌کد
r	Latin Small Letter R	U+0072	r	Latin Small Letter R	U+0072
p	Latin Small Letter P	U+0070	p	Latin Small Letter P	U+0070
n	Latin Small Letter N	U+006E	n	Latin Small Letter N	U+006E
e	Latin Small Letter E	U+0065	e	Latin Small Letter E	U+0065
g	Latin Small Letter G	U+0067	g	Latin Small Letter G	U+0067
a	**Latin Small Letter A**	**U+0061**	**a**	**Cyrillic Small Letter A**	**U+0430**
r	Latin Small Letter R	U+0072	r	Latin Small Letter R	U+0072

جدول ۱ هم‌نگاره‌ای نویسه‌های a لاتین و a سیریلیک در نام دامنه rpnegar.com

نحوه نمایش نویسه سیریلیک a	نحوه نمایش نویسه لاتین a	عنوان فونت
a	a	Arial
a	a	Calibri
a	a	Courier New
a	a	Exo 2
a	a	Segoe UI
a	a	Tahoma
a	a	Times New Roman

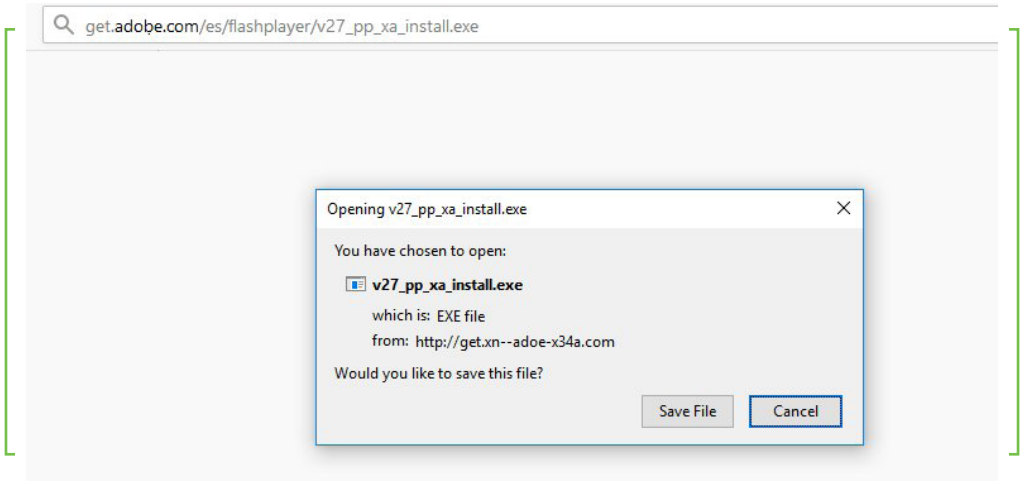
جدول ۲ هم‌نگاره‌ای نویسه‌های a لاتین و a سیریلیک در بسیاری از فونت‌ها

ماجرای یک حمله

در جریان یکی از حملات ماحیگیری هم‌نگاره سال‌های اخیر، مهاجمان اقدام به ثبت دامنه‌ای با نام adoḅe[.]com کردند. همان‌طور که پیداست با جایگزینی نویسه b با ḅ تلاش شده بود تا دامنه معتبر adobe.com به‌نحوی قابل‌باور جعل شود.

علاوه بر تشابه بالای دو نویسه b و ḅ، مهاجمان موفق شده بودند که دامنه مذکور را به نام Adobe Systems Incorporated ثبت کنند که خود عاملی دیگر در معتبر جلوه دادن این نشانی بود.

در زمان ورود کاربر به adoḅe[.]com، این‌طور وانمود می‌شد که برای نمایش صحیح محتوای وب‌سایت باید با کلیک بر روی لینک درج شده، یک به‌روزرسانی Adobe Flash Player بر روی دستگاه نصب شود. در صورت کلیک بر روی لینک و اجرای فایل دریافت شده، دستگاه به نسخه‌ای از بدافزار Beta Bot آلوده می‌شد.



شکل ۲ فایل ناقل بدافزار Beta Bot که از طریق سایت adoḅe[.]com کاربر تشویق به دریافت آن می‌شود [۲]

در زمان اجرای فایل مخرب Beta Bot، بدافزار اقدام به غیرفعال‌سازی نرم‌افزارهای امنیتی نصب شده بر روی دستگاه کرده و دسترسی کاربر به وب‌سایت‌های امنیتی را محدود می‌کند. در ادامه، در انتظار دریافت فرامین از سوی گردانندگان خود می‌ماند.

از جمله قابلیت‌های Beta Bot می‌توان به سرقت داده‌های قربانی و استخراج رمز ارز[۱] با استفاده از منابع دستگاه تسخیر شده اشاره کرد.

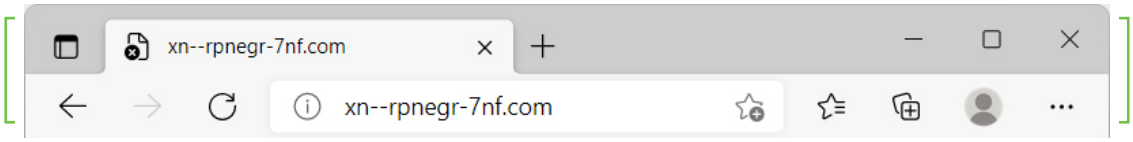
[۱] Cryptocurrency Mining

>_ پانی‌کد؛ مبدلی که می‌تواند راهکار باشد

پانی‌کد[1]، چهارچوبی در یونی‌کد است که از آن برای تبدیل نویسه‌های غیرلاتین نام‌های دامنه به رشته‌هایی متشکل از نویسه‌های لاتین استفاده می‌شود. به بیان ساده‌تر هر نویسه غیرلاتین دارای شناسه‌ای است که از تعدادی نویسه لاتین تشکیل شده است.

برای مثال، «xn--ngb» پانی‌کد حرف «ب» است. یا در مثالی دیگر، کلمه آلمانی «München» که حرف دوم آن نویسه‌ای غیرلاتین است در پانی‌کد به‌صورت «xn--mnchen-3ya» کدگذاری می‌شود.

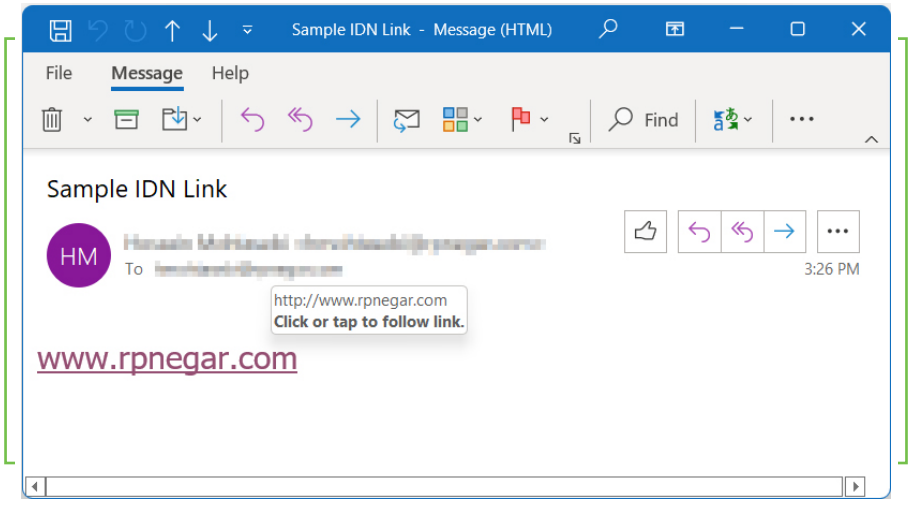
اکثر مرورگرها[2]، بر اساس سیاست‌های خود که در بخش بعدی به برخی از آنها پرداخته شده، نویسه‌های غیرلاتین دامنه‌های مشکوک را در نوار نشانی[3] به‌صورت پانی‌کد نمایش می‌دهند. بدین‌ترتیب فراخوانی نشانی «rpnegar.com» که در آن از نویسه سیریلیک a استفاده شده است منجر به تبدیل آن به «http://xn--rpnegr-7nf.com» در نوار نشانی مرورگر می‌شود.



شکل ۳ نمایش نشانی حاوی نویسه سیریلیک در قالب پانی‌کد

بنابراین تغییر نام دامنه در نوار نشانی مرورگر و تبدیل آن به نامی متفاوت از دامنه مورد نظر می‌تواند نشانه‌ای از مخرب بودن آن باشد.

لازم به ذکر است که نمایش نام دامنه در قالب پانی‌کد به‌صورت پیش‌فرض در نرم‌افزار Outlook برقرار نیست و اگر کاربر، موشواره را بر روی لینک دامنه مذکور نگاه دارد، در Tooltip، نام دامنه کاملا معتبر به نظر می‌رسد؛ موضوعی که می‌تواند احتمال کلیک کاربر بر روی لینک مخرب را به طور چشمگیری افزایش دهد.



شکل ۴ عدم نمایش نام دامنه حاوی نویسه غیرلاتین در قالب پانی‌کد در Tooltip نرم‌افزار Outlook

[1] Punycode
[2] Browser
[3] Address bar

>_ اینترنت چندزبانی یا چشم‌پوشی از IDN بخاطر ریسک آن؟ مسأله این است!

هدف از معرفی و پیاده‌سازی ثبت نام‌های دامنه بین‌المللی یا همان IDN، چندزبانی کردن بستر اینترنت بوده است. در عین حال تبدیل همیشگی نویسه‌های غیرلاتین دامنه به پانی‌کد، اگر چه از نگاه امنیتی اقدامی مثبت است اما با رویکردی موجب پیدایش IDN شد همخوانی ندارد.

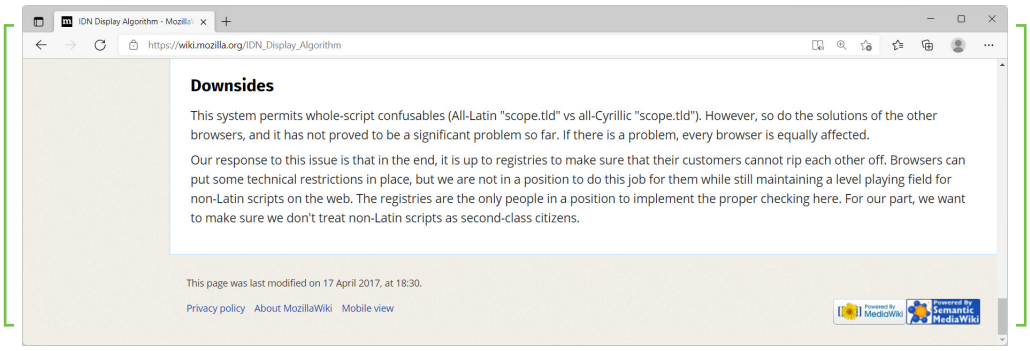
در سال‌های گذشته شرکت‌های سازنده مرورگر هر کدام با بکارگیری الگوریتم‌های خاص تلاش کرده‌اند تا تبدیل نویسه‌های غیرلاتین یک نام دامنه بین‌المللی به پانی‌کد را محدود به موارد مشکوک کنند. سیاست‌های برخی از این شرکت‌های سازنده در ادامه قابل مطالعه است.

مرورگرهای مبتنی بر Chromium شامل Google Chrome، Microsoft Edge و Opera:
https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md

مرورگر Mozilla Firefox:
https://wiki.mozilla.org/IDN_Display_Algorithm

مرورگر Safari:
https://support.apple.com/kb/TA22996?locale=en_US

باید در نظر داشت که هیچ‌یک از الگوریتم‌های فعلی قادر به کشف تمامی نام‌های دامنه هم‌نگاره نیستند؛ بسیاری از کارشناسان معتقدند که این، نهادهای ثبت‌کننده دامنه هستند که می‌بایست کنترل‌های صحیحی به‌منظور جلوگیری از ساخت دامنه‌های هم‌نگاره اعمال کنند.



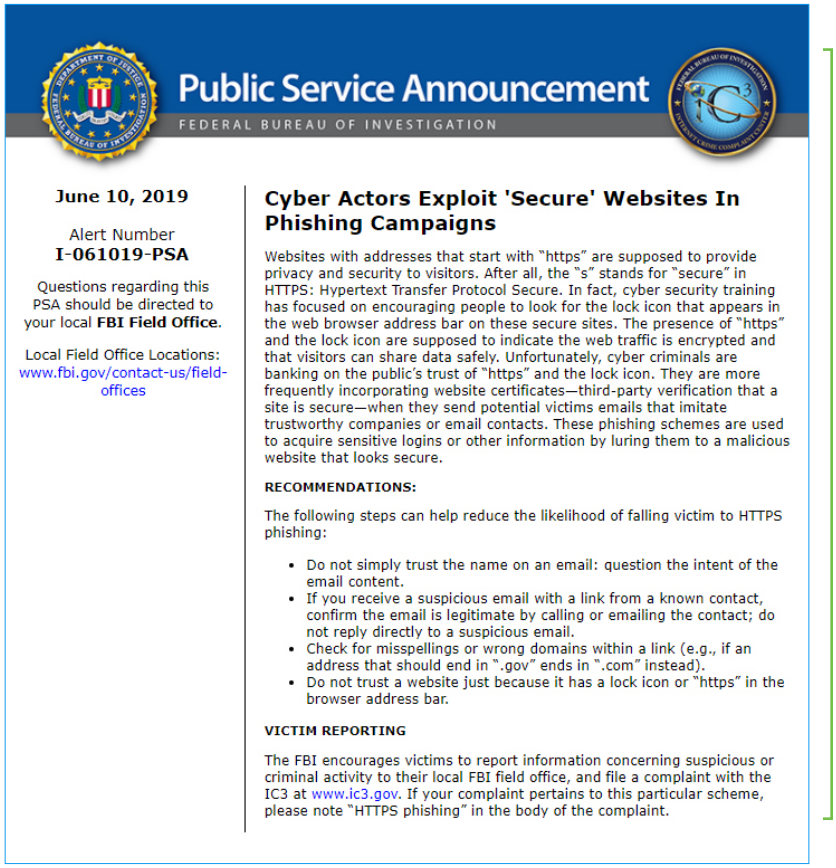
شکل ۵ اشاره Mozilla به نقش کلیدی نهادهای ثبت‌کننده دامنه در جلوگیری از ساخت دامنه‌های هم‌نگاره

>_ باوری نادرست

یکی از باورهای نادرست در میان کاربران، معتبر پنداشتن هر نام دامنه و وب‌سایتی است که از پودمان رمزگذاری HTTPS استفاده می‌کند. این در حالی است که بر اساس گزارشی که شرکت Bitdefender در آبان ۱۴۰۰ آن را منتشر کرد ۹/۴٪ از وب‌سایت‌های جعلی هم‌نگاره از پودمان HTTPS استفاده می‌کنند [۳].

شاید یکی از اصلی‌ترین دلایل در پیدایش این باور، نمایش قفل سبز رنگ[۱] در زمان مراجعه به این وب‌سایت‌ها باشد. اما باید توجه داشت نشان مذکور فقط نمایانگر محرمانه بودن ارتباطات میان کاربر و آن وب‌سایت است و نه چیز دیگر.

پیش‌تر نیز مرکز IC3 ایالات متحده[۲] نسبت به گسترش حملات ماحیگیری از طریق وب‌سایت‌های با پودمان HTTPS هشدار داده بود.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 10, 2019

Alert Number
I-061019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Cyber Actors Exploit 'Secure' Websites In Phishing Campaigns

Websites with addresses that start with "https" are supposed to provide privacy and security to visitors. After all, the "s" stands for "secure" in HTTPS: Hypertext Transfer Protocol Secure. In fact, cyber security training has focused on encouraging people to look for the lock icon that appears in the web browser address bar on these secure sites. The presence of "https" and the lock icon are supposed to indicate the web traffic is encrypted and that visitors can share data safely. Unfortunately, cyber criminals are banking on the public's trust of "https" and the lock icon. They are more frequently incorporating website certificates—third-party verification that a site is secure—when they send potential victims emails that imitate trustworthy companies or email contacts. These phishing schemes are used to acquire sensitive logins or other information by luring them to a malicious website that looks secure.

RECOMMENDATIONS:

The following steps can help reduce the likelihood of falling victim to HTTPS phishing:

- Do not simply trust the name on an email: question the intent of the email content.
- If you receive a suspicious email with a link from a known contact, confirm the email is legitimate by calling or emailing the contact; do not reply directly to a suspicious email.
- Check for misspellings or wrong domains within a link (e.g., if an address that should end in ".gov" ends in ".com" instead).
- Do not trust a website just because it has a lock icon or "https" in the browser address bar.

VICTIM REPORTING

The FBI encourages victims to report information concerning suspicious or criminal activity to their local FBI field office, and file a complaint with the IC3 at www.ic3.gov. If your complaint pertains to this particular scheme, please note "HTTPS phishing" in the body of the complaint.

شکل ۶ هشدار مرکز IC3 در خصوص گسترش حملات ماحیگیری از طریق وب‌سایت‌های با پودمان HTTPS

[۱] Green Padlock
[۲] US Internet Crime Complaint Center

< جمع‌بندی />

تشخیص تهدیدات ماحیگیری هم‌نگاره از نوع ثبت دامنه بین‌المللی، برای کاربران حتی افراد حرفه‌ای و باتجربه بسیار دشوار است. اگر چه با سازوکارهای پیاده‌سازی شده توسط مرورگرها شاید بتوان به بی‌اثر شدن نمونه‌های نه‌چندان پیچیده آنها امید بست اما در هر صورت ریسک این تهدیدات که خود می‌توانند درگاهی برای ورود مهاجمان به شبکه سازمان و سرآغاز امور مخربی همچون سرقت اطلاعات، انتشار باج‌افزار[1] و... باشند باید به‌طور جدی در نظر گرفته شود.

در سال‌های اخیر افزونه‌هایی[2] نیز برای برخی مرورگرها به‌منظور غیرفعال کردن دسترسی به وب‌سایت‌های با نام دامنه بین‌المللی عرضه شده که استفاده از آنها می‌تواند به‌نحوی مؤثر این تهدیدات را خنثی کند. آموزش کارکنان نیز نقشی کلیدی در مقابله با این تهدیدات پیشرفته دارد.

و در آخر، اگر از راهبران و مسئولان امنیت سازمانتان هستید، استفاده از محصول آروید را برای ایمن ماندن کاربرانتان از گزند تهدیدات مبتنی بر مهندسی اجتماعی به شما توصیه می‌کنیم. اطلاعات بیشتر در خصوص این محصول را در نشانی www.rpnegar.com دریافت کنید.

[1] Ransomware
[2] Browser Extension

منابع

[۱] Mimoso, Michael (2017-09-06). "IDN Homograph Attack Spreading Betabot Backdoor". *Threatpost*. Retrieved 2022-01-25.

[۲] Ankit Anubhav [@ankit_anubhav] (2018-05-23). "ḅ vs b !" (Tweet) – via Twitter.

[۳] Zugec, Martin (2021-10-28). "Bitdefender Threat Debrief | October 2021". *Bitdefender*. Retrieved 2022-01-14.

[۴] "HTTPS Protocol Now Used in 58% of Phishing Websites". *Trend Micro*. 2019-06-24. Retrieved 2022-01-26.

[۵] Gatlan, Sergiu (2019-06-10). "FBI Issues Warning on 'Secure' Websites Used For Phishing". *Bleeping Computer*. Retrieved 2022-01-26.

[۶] "Cyber Actors Exploit 'Secure' Websites In Phishing Campaigns". *The Internet Crime Complaint Center (IC3)*. 2019-06-10. Retrieved 2022-01-26.

Acknowledgement

RPNegar acknowledges Vecteezy and Pixabay as well as their members for providing some images included in this report.

درباره ما

شرکت رامونا پردازش نگار، اولین و تنها ارائه‌دهنده محصولات شبیه‌ساز تهدیدات مبتنی بر مهندسی اجتماعی در ایران است. متخصصان ما ضمن رصد و تحلیل جدیدترین بدافزارها و حملات سایبری که از تکنیک‌های مهندسی اجتماعی برای به دام انداختن کاربران و رخنه به شبکه سازمان‌ها بهره می‌گیرند با همکاری با بخش تولید به‌طور مستمر در حال بهبود و تکامل محصولات رامونا پردازش نگار هستند تا سازمان‌ها و کسب‌وکارهای ایرانی از گزند این تهدیدات روزافزون در امان باشند. ما به آنچه می‌کنیم ایمان داریم و باافتخار برای ساخت محصولاتی پیشرو در حوزه امنیت فناوری اطلاعات در کنار ارائه خدماتی شایسته مشتریان ارزشمندمان همواره تلاش می‌کنیم.

www.rpnegar.com info@rpnegar.com ۹۱۰۳۱۹۷۳ @rpnegar @rpnegar @rpnegar