گزارش آسیب‌پذیری CVE-2020-1350

شرح آسیب‌پذیری SIGRed در سرویس DNS سرور ویندوز

و نحوه رفع آن

شماره گزارش VU00401

تیر ۱۳۹۹

گروه امنیت سایبری
امن‌بان
AMN BAN
CYBER SECURITY GROUP

تهران، آزادراه تهران ـ کرج، بلوار چوگان، روبروی شهرک آزادی، پردیس نوآوری شهید مقدم، واحد ۸

۰۲۱ - ۲۸۴۲۴۴۶۳

www.AmnBan.ir

بسم الله الرحمن الرحیم

AMN BAN

گروه امنیت سایبری امن‌بان

گروه امنیت سایبری
امن‌بان
AMN BAN
CYBER SECURITY GROUP

فهرست

۰- حق چاپ و نشر

این مستند گزارش آسیب‌پذیری است که توسط شرکت «امن‌بان فناوری‌شریف» تهیه شده است.

رفع مسئولیت

شرکت «امن‌بان فناوری‌شریف» هیچگونه مسئولیتی در قبال سوء استفاده یا مشکلات استفاده از این گزارش ندارد و کلیه مسئولیت بر عهده استفاده کننده می‌باشد.

کپی رایت

کلیه حقوق مادی و معنوی این مستند متعلق به شرکت «امن‌بان فناوری‌شریف» بوده و محفوظ می‌باشد. هرگونه نسخه برداری از قبیل رونوشت، ترجمه بخش یا بخش هایی از آن فقط با اخذ مجوز کتبی از «امن‌بان» امکان‌پذیر می‌باشد.

۱- شروع ماجرا

در روزهای گذشته خبر آسیب‌پذیری با شناسه CVE-2020-1350 و با نام SIGRed در سرویس DNS سیستم عامل ویندوز توسط شرکت Check Point[۱] منتشر شد.

سرویس DNS سرویسی است که وظیفه تبدیل نام دامنه به آدرس IP را دارد و در شبکه‌های مبتنی بر محصولات Microsoft یکی از سرویس‌های حیاتی است. آسیب‌پذیری SIGRed که دارای امتیاز CVSS 10 (بالاترین امتیاز ممکن) است که در تمام نسخه‌های ویندوز سرور از ۲۰۰۳ تا ۲۰۱۹ وجود دارد. بهره‌جویی[۲] این آسیب‌پذیری از راه دور قابل انجام است و نیاز به هیچ گونه احراز هویت ندارد. مهاجم به کمک این آسیب‌پذیری می‌تواند به دسترسی Domain Admin هم دست پیدا کند.

در این گزارش به زبان ساده خطرات این آسیب‌پذیری، نحوه بررسی آسیب‌پذیر بودن سیستم و به روزرسانی آن را شرح خواهیم داد.

۲- آسیب‌پذیری CVE-2020-1350 چه آثار مخربی دارد؟

این آسیب‌پذیری چون به مهاجم دسترسی Domain Admin می‌دهد که دسترسی بسیار بالایی در شبکه‌های ویندوزی است و مهاجم به کمک این دسترسی عملاً می‌تواند علاوه بر سرور DNS آسیب پذیر روی تمام سیستم‌های عضو دامنه نیز دسترسی پیدا کند، بسیار مخرب است.

۳- آیا سیستم من آسیب‌پذیر است؟

برای بررسی آسیب پذیر بودن یک سیستم، فعلا هیچ ابزار مطمئنی منتشر نشده است که به محض انتشار در نسخه جدید این گزارش منتشر خواهد شد.

۴- نحوه مقابله

برای مقابله با این آسیب‌پذیری باید ویندوز خود را طبق یکی از روش‌های زیر به روز رسانی کنید.

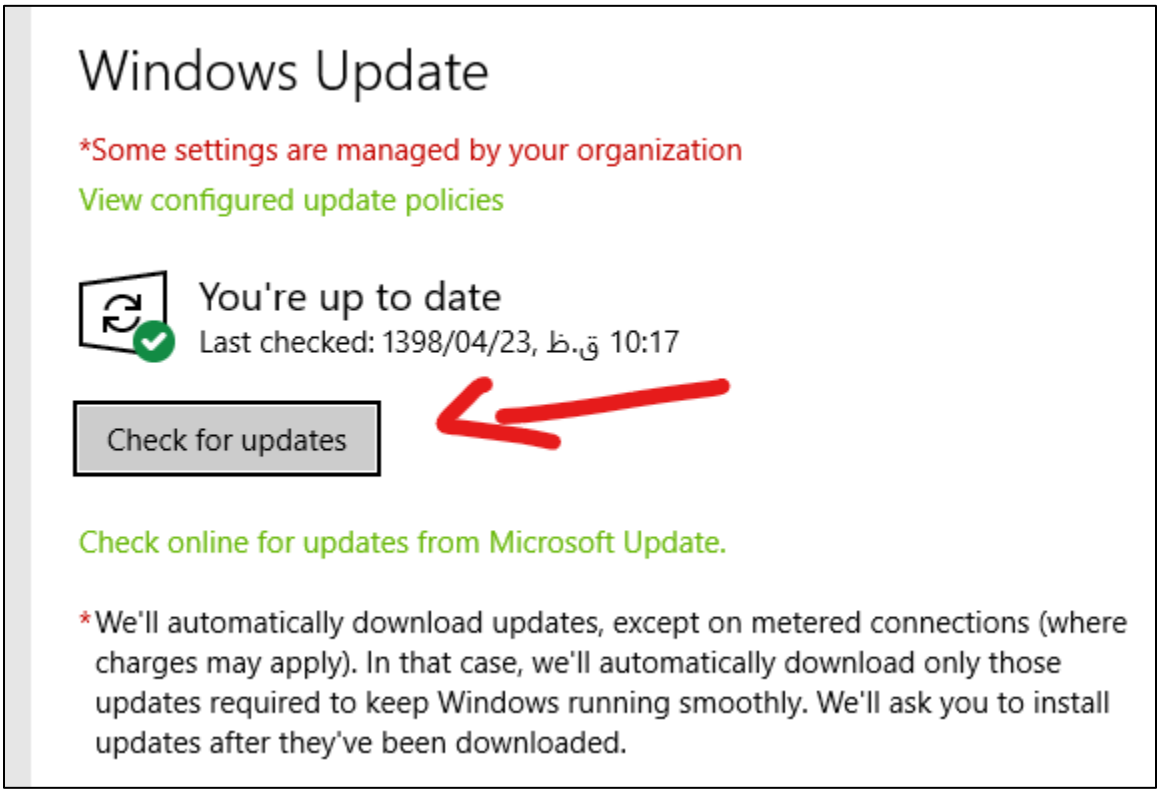
۴-۱- روش اول ـ به روزرسانی خودکار (توصیه می شود)

سیستم خود را به اینترنت متصل کنید و در منوی استارت ویندوز update را تایپ کنید و روی windows update و در صفحه بازشده Check for updates (شکل ۱) کلیک کنید و مدت طولانی منتظر بمانید تا ویندوز شما آپدیت شود و درنهایت سیستم را Restart کنید.

---

[۱] https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/

[۲] Exploit



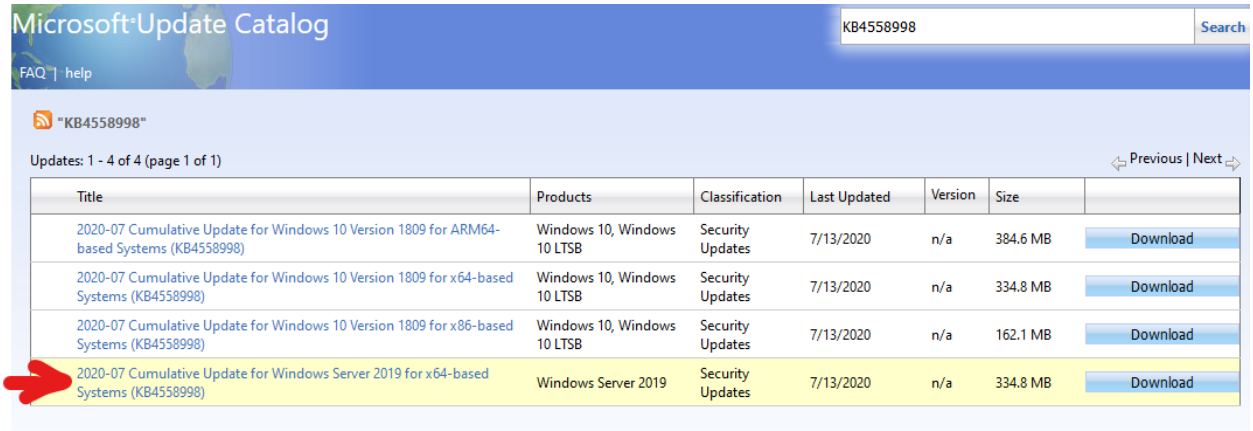
شکل ۱- شروع بروزرسانی ویندوز

۲-۴- روش دوم ـ به روزرسانی دستی

اگر به هر دلیلی امکان به روزرسانی خودکار برای شما وجود ندارد از این روش استفاده کنید.

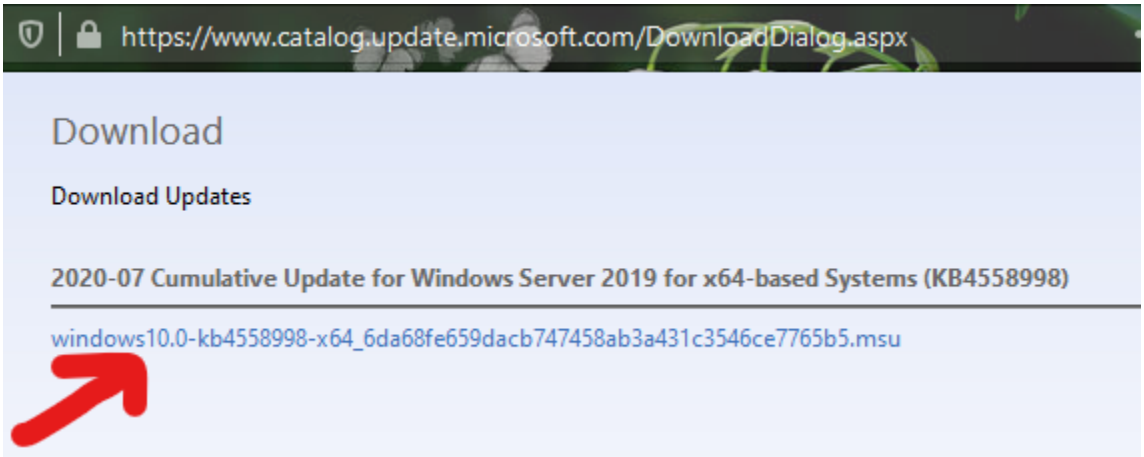
ابتدا با نوشتن winver در run یا منو استارت ویندوز نسخه دقیق ویندوز را تعیین کنید. پس از تعیین نسخه دقیق ویندوز به صفحه توضیحات آسیب‌پذیری بروید و در بخش Security Updates متناسب با نسخه ویندوز خود آپدیت مناسب را انتخاب کنید و با کلیک روی Security Update به صفحه دانلود به روزرسانی بروید.

در صفحه دانلود بازهم متناسب با نسخه ویندوز خود روی دکمه Download کلیک کنید (شکل ۲).



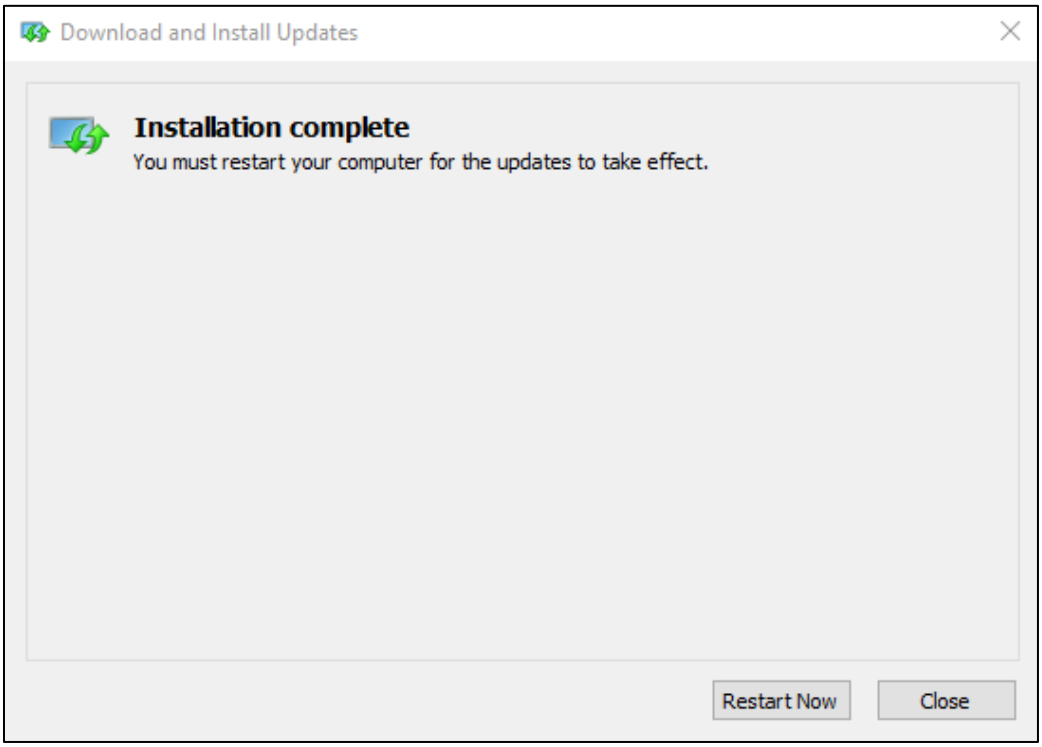
شکل ۲- صفحه دانلود آپدیت

در صفحه باز شده روی لینک آپدیت مورد نظر (شکل ۳) کلیک کنید تا دانلود فایل آغاز شود.



شکل ۳- لینک دانلود آپدیت

پس از دانلود، فایل دریافتی که با نامی مشابه windows10.0-kbxxx-xxxxxxxxxxxxxx.msu است را اجرا کنید و روی Yes کلیک کنید تا نصب آپدیت آغاز شود. در پایان پیام شکل ۴ نمایش داده می‌شود و روی Restart Now کلید کنید تا نصب تکمیل شود.



شکل ۴- پایان نصب آپدیت

۳-۴- روش سوم – غیرفعال کردن به کمک رجیستری

در صورتی که زمان کافی ندارید و یا به هردلیلی نمی‌توانید از روش‌های بالا ویندوز را آپدیت کنید به کمک تغییر در یک کلید رجیستری می‌توانید جلوی این آسیب‌پذیری را بگیرید[۳].

به مسیر زیر در رجیستری سرور بروید:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters

کلید رجیستری زیر که از نوع DWORD است را بیابید:

TcpReceivePacketSize

مقدار آن را به مقدار زیر تغییر دهید. مقدار اولیه آن (0xFFFF) است[۴].

0xFF00

سرویس DNS را Restart کنید.

---

[۳] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

[۴] https://support.microsoft.com/en-us/help/4569509/windows-dns-server-remote-code-execution-vulnerability

با اجرای دستورات زیر در CMD که به صورت Run as admin اجرا شده باشد هم می‌توان کارهای فوق را انجام داد.

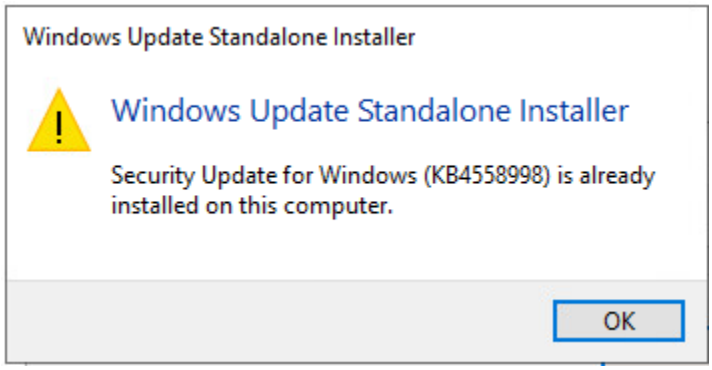
```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" /v "TcpReceivePacketSize" /t REG_DWORD /d 0xFF00 /f

net stop DNS && net start DNS
```

۵- بررسی نصب بودن به روزرسانی

با روش‌های زیر از نصب به روزرسانی اطمینان حاصل کنید.

۵-۱- روش اول

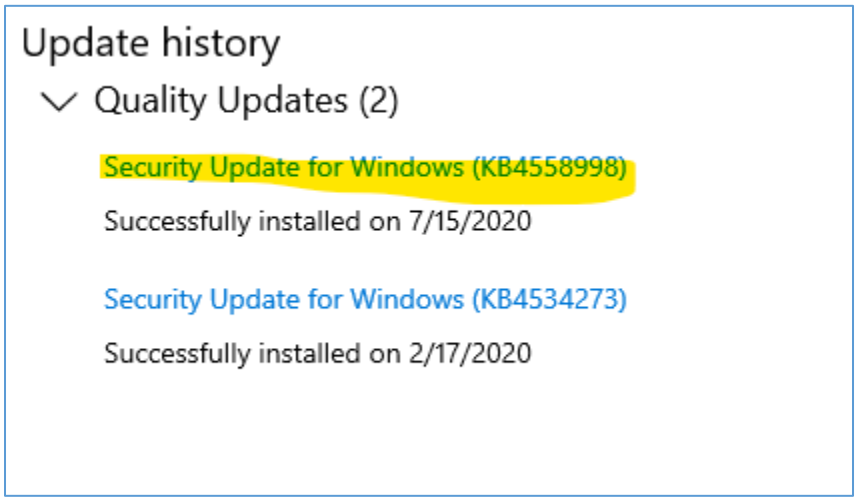
فایل نصب آپدیت را دوباره اجرا کنید اگر نصب باشد به شما پیام شکل ۵ نمایش داده می‌شود 😊.



شکل ۵- پیام نصب بودن آپدیت

۵-۲- روش دوم

برای بررسی نصب بودن به روزرسانی روی یک سیستم update history را در منو استارت ویندوز تایپ کنید و در برگه View update history به دنبال نام آن مثلاً KB4558998 بگردید (شکل ۶). توجه داشته باشید که بسته به نسخه ویندوز ممکن است نام به‌روزرسانی متفاوت باشد. مثلاً برای ویندوز 2004 نام به روزرسانی KB4565503 است این نام را در ابتدای نام فایل به روزرسانی دانلود شده می توانید ببینید در جدول ۱ نام آپدیت‌ها بر اساس نسخه ویندوز آورده شده است.



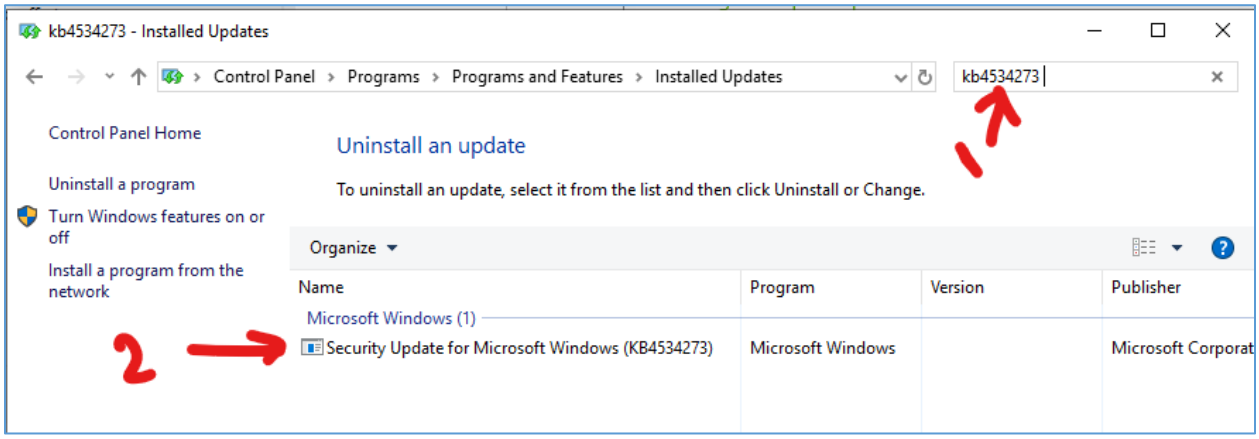
شکل ۶- بررسی نصب آپدیت

جدول ۱- جدول نام آپدیت‌ها بر اساس نسخه ویندوز

Product	KB Name
Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)	4565536 or 4565529
Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	4565524 or 4565539
Windows Server 2012 Windows Server 2012 (Server Core installation)	4565537 or 4565535
Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation)	4565541 or 4565540
Windows Server 2016 Windows Server 2016 (Server Core installation)	4565511
Windows Server 2019 Windows Server 2019 (Server Core installation)	4558998
Windows Server, version 1903 (Server Core installation) Windows Server, version 1909 (Server Core installation)	4565483
Windows Server, version 2004 (Server Core installation)	4565503

۵-۳- روش سوم

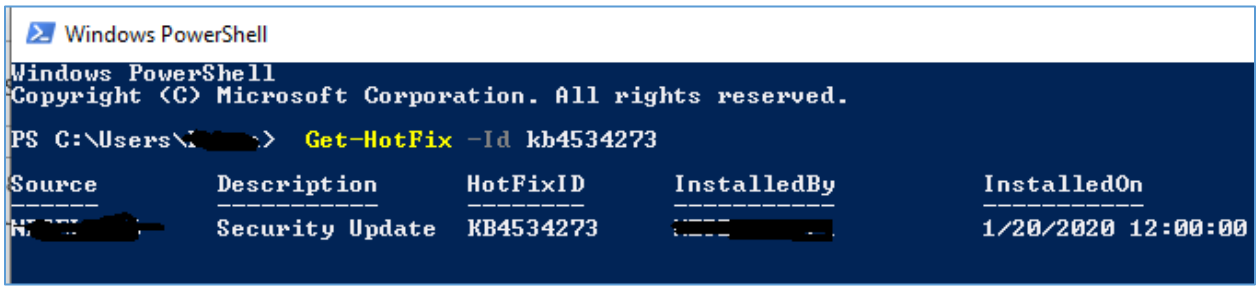
در منوی استارت appwiz.cpl را تایپ کنید و آن را اجرا نمایید در سمت چپ روی View installed updates کلیک کنید در این صفحه دنبال آپدیت بگردید، از قسمت جستجوی بالا هم می‌توانید کمک بگیرید (شکل ۷).



شکل ۷–بررسی نصب آپدیت روش دوم

۵-۴- روش چهارم (حرفه‌ای)

در powershell دستور Get-HotFix –Id با نام مناسب KB (طبق جدول ۱) را وارد کنید اگر آپدیت نصب شده باشد خروجی باید به شکل ۸ باشد وگرنه پیام خطا نمایش داده می‌شود.



شکل ۸– بررسی نصب با **PowerShell**

۶- سوالات متداول

آیا این آسیب‌پذیری روی کلاینت‌ها هم تاثیری دارد؟

خیر، این آسیب‌پذیری فقط مربوط به سروری است که روی آن سرویس DNS در حال اجراست.

تا آسیب‌پذیری جدید بدرود! ☺

درباره ما:

گروه امنیت سایبری امن‌بان به همت جمعی از فارغ التحصیلان دانشگاه صنعتی شریف در سال ۱۳۹۷ با هدف آگاهی رسانی، تحقیق و پژوهش در جهت ارتقای امنیت سایبری کشور تشکیل شد. فعالیت این گروه به صورت رسمی از سال ۱۳۹۸ با ثبت شرکت امن‌بان فناوری‌های پیشرفته شریف با شماره ثبت ٥٤٤٨٩٤ و اخذ مجوز از مراجع ذی صلاح با نام تجاری امن‌بان ادامه یافت. همچنین مجموعه امن‌بان با کد عضویت ۲۱۰۱۳۸۸۰ عضو نظام صنفی رایانه‌ای استان تهران می‌باشد.

تماس با ما:

۰۲۱-۲۸۴۲۴۴۶۳

https://amnban.ir

mail@amnban.ir

شبکه‌های اجتماعی:

t.me/amnban

what.sapp.ir/AmnBAN

ble.ir/amnban

instagram.com/AmnBan