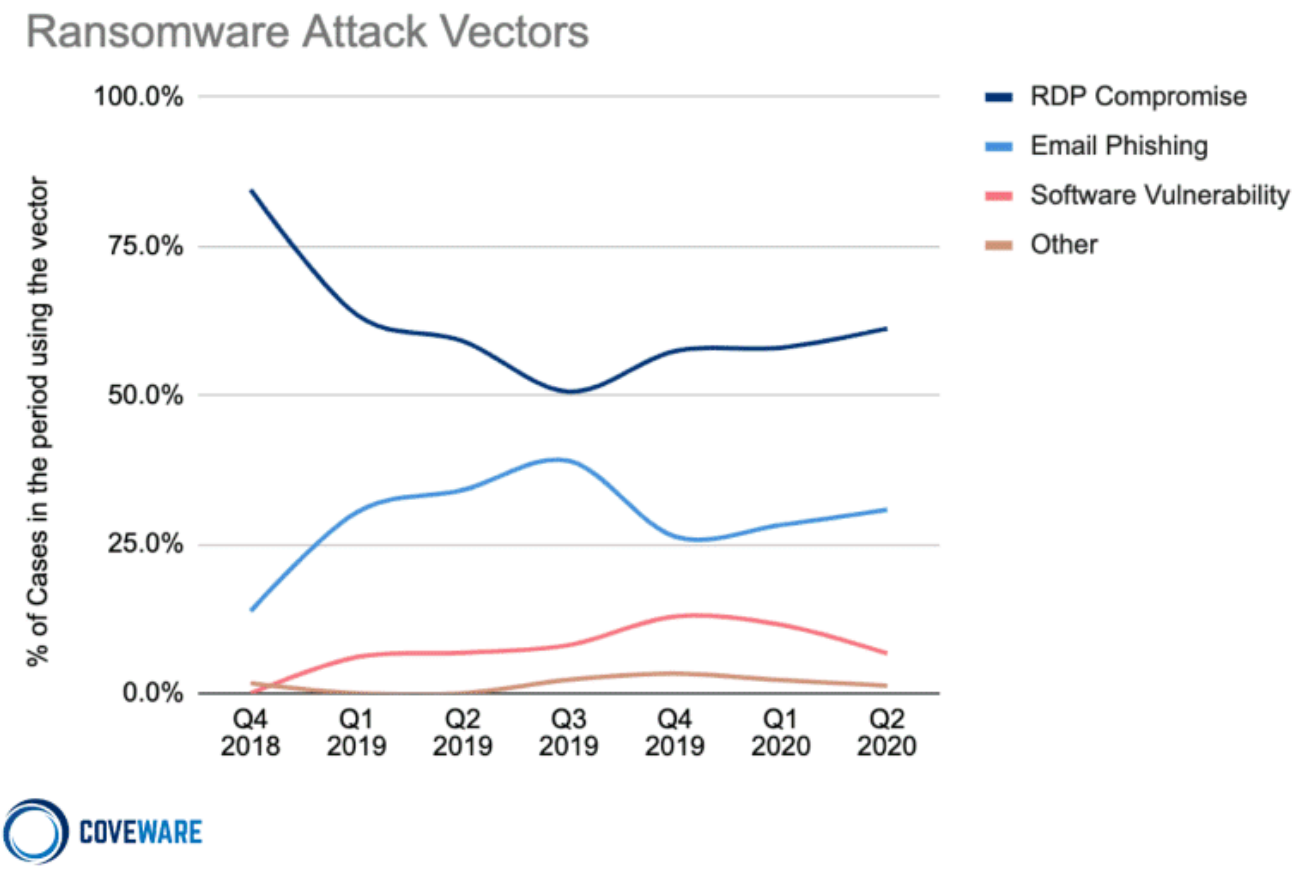
افزایش بی‌سابقه حملات باج‌افزاری در نیمه اول ۲۰۲۰؛ سو استفاده از VPN روش محبوب هکرها - دیجیاتو

پیمان حسنی | دوشنبه، ۰۳ شهریور ۱۳۹۹

گزارش جدید نشان می‌دهد حملات باج افزاری به شرکت‌ها در نیمه اول سال ۲۰۲۰ رشد بی‌سابقه‌ای داشته‌اند. پروتکل ریموت دسکتاپ (RDP)، فیشینگ و سواستفاده از VPN، سه مسیر مورد علاقه هکرها برای نفوذ به سیستم قربانی در بازه یاد شده بوده‌اند.

به گزارش ZDnet، پروتکل دسترسی از راه دور به دسکتاپ (RDP)، محبوب ترین مسیر نفوذ به سیستم قربانیان و عامل اصلی بیشتر حملات باج افزاری در سال ۲۰۲۰ بوده است. چندین شرکت امنیت سایبری با انتشار گزارشاتی جداگانه این موضوع را تأکید کرده‌اند.

شرکت Emsisoft ماه گذشته میلادی اعلام کرد RDP بزرگترین مسیر نفوذ به سیستم قربانی (attack vector) در حملات باج افزاری بوده است. آمارهای شرکت امنیتی Coveware نیز نشان می‌دهند در سال جاری میلادی پروتکل ریموت دسکتاپ محبوب ترین مسیر دسترسی به سیستم قربانی در حملات باج افزاری بوده است. در گزارش شرکت Recorded Future نیز RDP در صدر لیست قرار گرفته است.



سو استفاده از VPN و شبکه‌های مشابه، روش مورد علاقه دیگر هکرها برای انجام حملات باج افزاری در سال ۲۰۲۰ بوده است. هکرها با سواستفاده از آسیب پذیری VPN به شبکه شرکت‌ها نفوذ کرده و بسته به تخصص و توانمندی، اقدامات خرابکارانه‌ای همچون جاسوسی از کشورها یا سرقت پول را انجام داده و یا نام کاربری و رمزعبور دسترسی به سیستم‌ها را به هکرهای دیگر فروخته‌اند.

سیستم‌های شرکت Citrix و سرورهای Pulse Secure VPN از اهداف مورد علاقه هکرها در حملات باج افزاری بوده‌اند. گروه‌های هک REvil (Sodinokibi), Ragnarok, DoppelPaymer, Maze, CLOP و Nefilim با استفاده از آسیب پذیری سیستم‌های Citrix در برابر باگ CVE-2019-19781 به شبکه قربانیان نفوذ کرده‌اند. همچنین گروه‌هایی همچون REvil و Black Kingdom با سواستفاده از آسیب پذیری سرورهای Pulse Secure VPN در برابر باگ CVE-2019-11510 به سیستم‌ها حمله کرده‌اند.

متخصصان امنیت سایبری برای کاهش احتمال حمله از طریق RDP و VPN به شرکت‌ها توصیه می‌کنند تا با نصب آخرین به‌روزرسانی‌های نرم افزاری امنیت شبکه را ارتقاء دهند.

[دیجیاتو]