ipsip VN

Báo cáo thử nghiệm Bảo mật nâng cao

FlexSecure 360

Email and Cloud Security

THG 5, 2025 | BẢO VỆ EMAIL

Giới thiệu

Tổng quan thử nghiệm

IPSIP Việt Nam đã thử nghiệm giải pháp FlexSecure360 Email and Cloud Security nhằm ứng phó với sự kết hợp của các cuộc tấn công có chủ đích sử dụng các kỹ thuật phổ biến và các cuộc tấn công công khai đang diễn ra trên Internet tại thời điểm thử nghiệm.

Kết quả cho thấy mức độ hiệu quả của giải pháp về khả năng phát hiện và/hoặc bảo vệ trước các mối đe dọa (threat) theo thời gian thực và trong khoảng thời gian ngắn sau khi các cuộc tấn công diễn ra.

Mục tiêu

Nhằm cung cấp một góc nhìn trung thực, khách quan và đầy đủ thông tin về khả năng phòng thủ của nền tảng bảo mật email trước những kẻ tấn công nhắm vào doanh nghiệp.

Báo cáo thử nghiệm Bảo mật nâng cao | Bảo vệ Email | FlexSecure360 Email and Cloud Security | Tháng 5, 2025

Giới thiệu về IPSIP Việt Nam

"Chứng nhận này khẳng định cam kết của công ty chúng tôi trong việc tuân thủ các tiêu chuẩn chuyên nghiệp, áp dụng các thực hành bảo mật tốt nhất và không ngừng cải tiến."

Nó phản ánh sự tận tụy của chúng tôi trong việc cung cấp các giải pháp đáng tin cậy, chất lượng cao và duy trì niềm tin với khách hàng cũng như đối tác.

Nếu bạn thắc mắc hoặc muốn thảo luận về chi tiết nào trong báo cáo này, vui lòng liên hệ với chúng tôi. IPSIP Việt Nam ứng dụng mô hình Threat Intelligence (Tình báo mối đe dọa) mới nhất nhằm đảm bảo các thử nghiệm của chúng tôi thực tế nhất có thể.

- **Thử nghiệm bảo mật email trước những kẻ tấn công nhắm vào doanh nghiệp:** Bỏ qua các kịch bản thử nghiệm Business Email Compromise sẽ mang lại nhiều rủi ro. Một thử nghiệm bảo mật tốt là phải thực tế, sử dụng các mối đe dọa được thấy trong đời thực.
- **Phòng thủ toàn diện:** Bảo mật email toàn diện đòi hỏi các biện pháp phòng thủ nhiều lớp tích hợp liền mạch với các nền tảng như Google Workspace hoặc Microsoft 365, cung cấp các khả năng phát hiện nâng cao.
- **Tiếp cận chủ động:** Bảo mật nên có tính thích ứng và chủ động, đảm bảo rằng tổ chức của bạn luôn được bảo vệ ngay cả khi các mối đe dọa phát triển.

Tóm tắt Tổng quan

Thử nghiệm này nhằm đánh giá tính hiệu quả của Coro Email and Cloud Security trước một loạt các mối đe dọa nhắm vào tập đoàn và doanh nghiệp nhỏ thông qua email. **IPSIP Việt Nam** đã sử dụng các kỹ thuật tấn công có mục tiêu nâng cao (APT) để xem xét khả năng xử lý các mối đe dọa an ninh mạng qua email của dịch vụ này.

Coro Email and Cloud Security	Điểm độ chính xác	Tỷ lệ (%)
Khả năng bảo vệ	4,545/4,860	94%
Tỷ lệ phát hiện threat	479/486	99%
Khả năng nhận biết tin hợp lệ	1,070/1,100	97%
Tổng độ chính xác	**5,615/5,960**	**94%**

Giải thưởng Thử nghiệm Bảo mật nâng cao

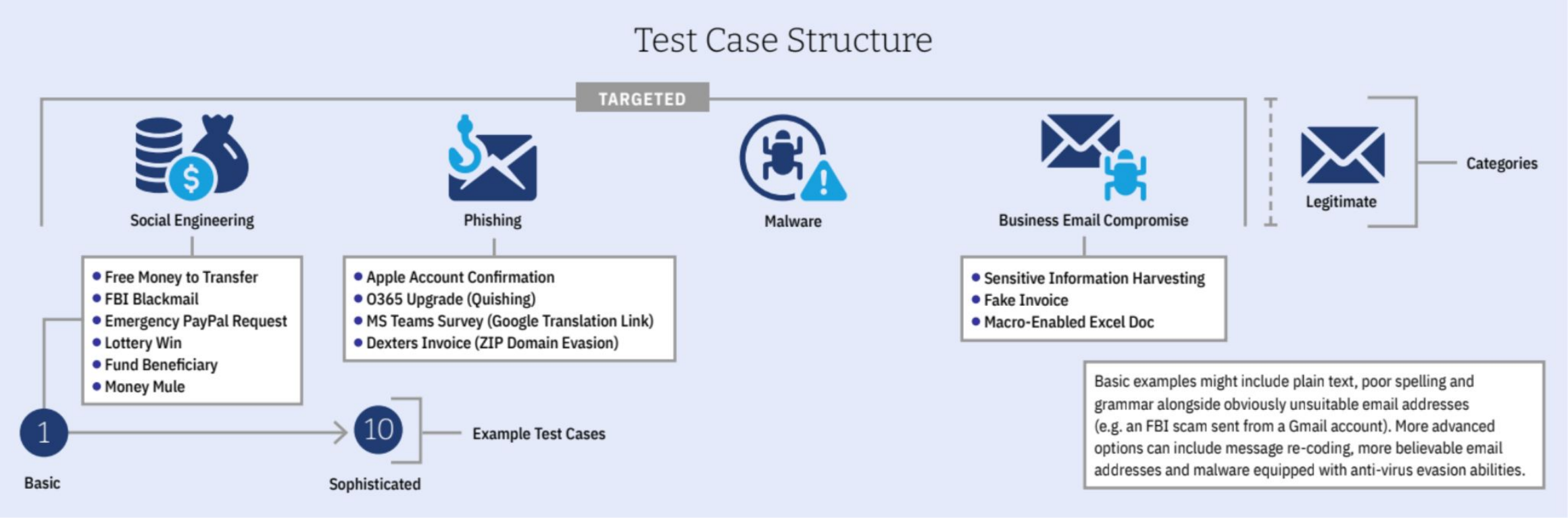
Hiệu năng xuất sắc

Coro Email and Cloud Security đã đạt được tỷ lệ Độ chính xác về khả năng bảo vệ tổng thể là 94%, chỉ bỏ sót một vài email có sử dụng các kỹ thuật Social Engineering và Business Compromise.

Những điểm số xuất sắc này đã đóng góp vào Tỷ lệ Tổng độ chính xác 94% và giải thưởng AAA dành cho Coro Email and Cloud Security.

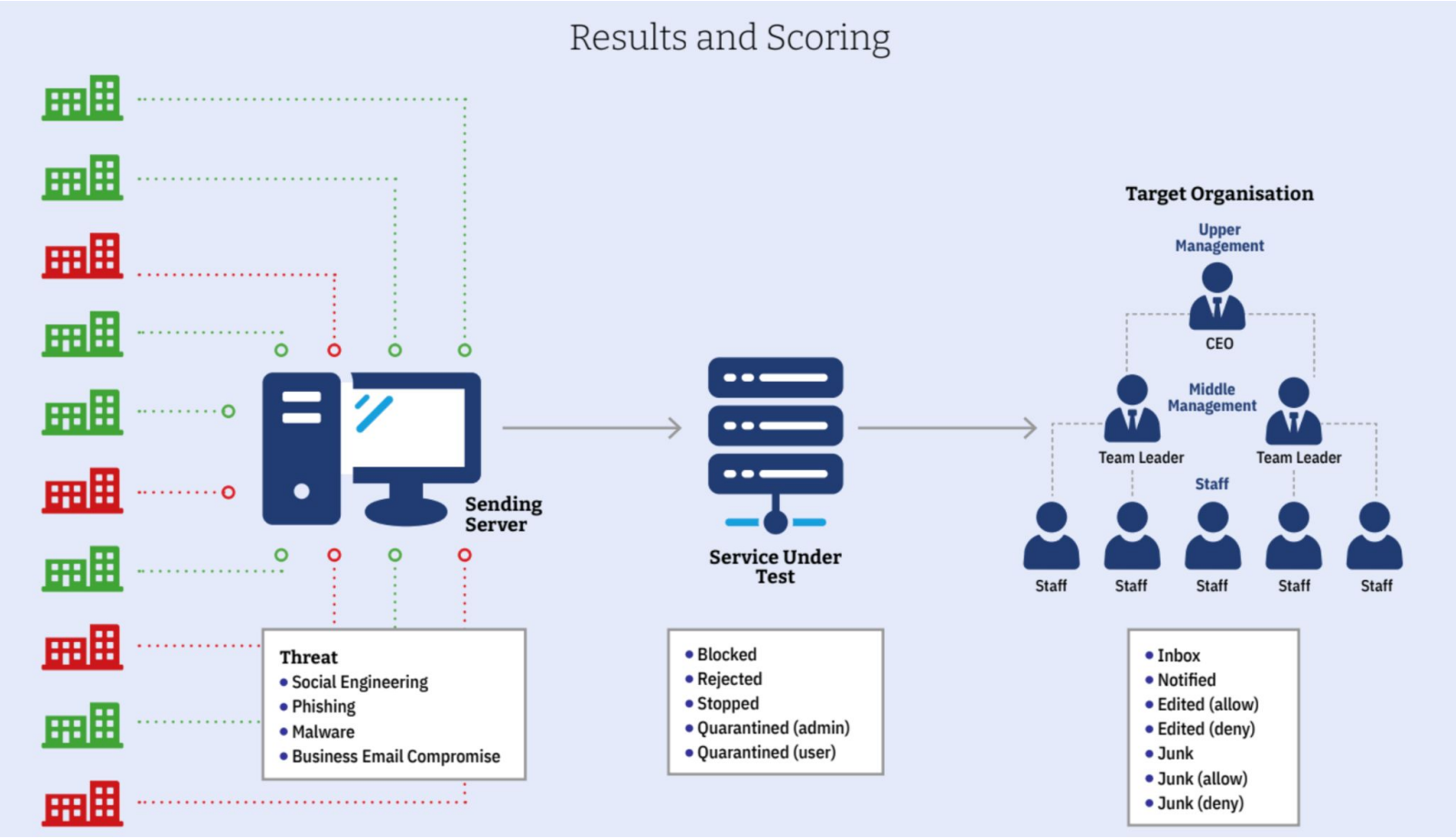
Chúng tôi đã thử nghiệm như thế nào?

Các cuộc tấn công có mục tiêu bao gồm bốn danh mục: Social Engineering; Phishing; Malware; và Business Email Compromise. Mục tiêu là kiểm tra tính hiệu quả của từng dịch vụ và cấu hình bảo mật email trước một loạt các loại tấn công khác nhau.



Cơ chế Ghi kết quả và Tính điểm

Các email được truyền qua internet đến người nhận. Trước khi vào được Hộp thư đến, chúng phải đi qua nhiều tầng dịch vụ bảo mật khác nhau để tiếp cận cơ sở hạ tầng của chính mục tiêu. Hoạt động phát hiện và bảo vệ có thể diễn ra ở nhiều giai đoạn.



Chi tiết tấn công

Khi thử nghiệm các dịch vụ phòng chống những cuộc tấn công có mục tiêu, việc đảm bảo các kịch bản tấn công được sử dụng sát với thực tế là điều vô cùng quan trọng. IPSIP Việt Nam sử dụng Threat Intelligence mới nhất để xem xét những phương thức tấn công đã được thực hiện trong vài năm qua và mô phỏng lại một cách sát sao.

Kẻ tấn công/ Nhóm APT	Phương thức	Chi tiết
OilRig	Trang web dẫn đến file .exe	Driveby-download đến một file .exe chứa Ransomware
Saint Bear	Link ẩn dẫn đến file .exe	Tài liệu PowerPoint độc hại chứa Ransomware
MuddyWater	Link ẩn dẫn đến file .exe	Tài liệu PDF độc hại chứa Ransomware
APT38	File .exe nén (.zip)	File .exe độc hại tạo một backdoor đến máy chủ C2
APT29	shellcode/exe	File .exe độc hại được nén zip tạo một backdoor đến máy chủ C2
Windshift	Link dẫn đến file .exe	File .exe độc hại tạo một backdoor đến máy chủ C2

Các lĩnh vực mục tiêu và phương thức tấn công

KEY					
	Critical Infrastructure		Defense		Energy
	Financial Industries		Government Espionage		Research Institutes

Attack Details

Attacker/ APT Group	Method	Target	Details
OilRig	Webpage to .exe		Drive-by download to an .exe file containing ransomware
Saint Bear	Hidden link to .exe		Malicious PowerPoint containing ransomware
MuddyWater	Hidden link to .exe		Malicious PDF document containing ransomware
APT38	Zipped exe		Malicious .exe file that creates a backdoor to a C2 server
APT29	shellcode/exe		Zipped malicious .exe file that creates a backdoor to a C2 server
Windshift	Link to .exe		Malicious .exe that creates a backdoor to a C2 server

1. Kết quả Khả năng phát hiện mối đe dọa

Mặc dù việc thử nghiệm và đánh giá các dịch vụ bảo mật email rất phức tạp, việc báo cáo các tỷ lệ phát hiện một cách rõ ràng vẫn có thể thực hiện được. Các số liệu dưới đây tóm tắt khả năng xử lý các mối đe dọa của mỗi dịch vụ và cấu hình theo cách tổng quát và cơ bản nhất.

Sản phẩm được thử nghiệm	Tỷ lệ phát hiện	Số lượng bỏ sót	Tỷ lệ phát hiện (%)
Coro Email and Cloud Security	479	7	**99%**

IPSIP Việt Nam GIỚI THIỆU THE-C2

The-C2 là một sự kiện độc quyền về Threat Intelligence, chỉ dành cho khách mời, kết nối các giám đốc điều hành doanh nghiệp đa quốc gia với những công nghệ tiên tiến nhất của ngành an ninh mạng.

Được tổ chức bởi **IPSIP Việt Nam**, sự kiện mang đến một hướng tiếp cận mới để thấu hiểu diễn biến của những mối đe dọa và các giải pháp bảo mật đang phát triển nhằm phòng thủ trước những kẻ tấn công.

2. Đánh giá Tổng độ chính xác

Đánh giá tính hiệu quả của một dịch vụ bảo vệ email hosting là một bài toán phức tạp và phải cân nhắc nhiều yếu tố. Hạng mục này không chỉ xem xét khả năng phát hiện và bảo vệ trước các mối đe dọa của từng dịch vụ, mà còn đánh giá cả cách xử lý những thông tin “không độc hại”.

Sản phẩm được thử nghiệm	Tổng độ chính xác	Tổng độ chính xác (%)
Coro Email and Cloud Security	**5,615/5,960**	**94%**

**Đánh giá Tổng độ chính xác kết hợp giữa Khả năng bảo vệ và ghi nhận các trường hợp False Positive.*

3. Đánh giá Khả năng bảo vệ và xử lý tin hợp lệ

- **Chặn; Từ chối; Thông báo; Can thiệp hiệu chỉnh (+10 cho threat;-10 cho tin hợp lệ):** Nếu dịch vụ phát hiện threat và chặn bất kỳ thành phần quan trọng nào của nó tiếp cận người nhận dự kiến, chúng tôi sẽ cộng 10 điểm.

- **Đưa vào thư mục Quarantine (Từ +6 đến +10 cho threat; -6 đến -10 cho tin hợp lệ):** Các dịch vụ can thiệp và chuyển các tin độc hại vào thư mục Quarantine sẽ được cộng điểm tùy thuộc vào việc người dùng hoặc quản trị viên (QTV) có thể khôi phục tin đó hay không.

- **Đưa vào thư mục Junk (+5 cho threat; -5 cho tin hợp lệ):** Tin được chuyển đến thư mục Junk của người dùng.

- **Hộp thư đến (-10 cho threat; +10 cho tin hợp lệ):** Mỗi trường hợp tin độc hại vượt qua được hệ thống bảo mật và lọt vào Hộp thư đến của người dùng sẽ bị trừ 10 điểm. Tất cả các tin hợp lệ được định tuyến chính xác sẽ được cộng 10 điểm.

Thể lệ tính điểm các kết quả khác

Hành động	Threat	Tin hợp lệ
Hộp thư đến	-10	10
Thư mục Junk	5	-5
Thư mục Quarantine (QTV)	10	-10
Thư mục Quarantine (Người dùng)	6	-6
Thông báo	10	-10
Buộc dừng	10	-10
Từ chối	10	-10
Chặn	10	-10
Hiệu chỉnh (Cho phép)	-10	10
Hiệu chỉnh (Từ chối)	10	-10
Thư mục Junk (Từ chối)	10	-10
Thư mục Junk (Cho phép)	-7	7

Công thức tính điểm đánh giá tổng quát

Đánh giá Khả năng bảo vệ

```
Protection rating =
(10 x number of Stopped etc.) +
(6-10 x number of Quarantined) +
(5 x number of Junk) +
(-10 x number of Inbox)
etc.
```

Đánh giá Khả năng nhận biết tin hợp lệ

```
Legitimate rating =
(10 x number of Inbox) +
(-5 x number of Junk) +
(-6-10 x number of Quarantined) +
(-10 x number of Stopped etc.)
etc.
```

Các hạng mục này dựa trên đánh giá của chúng tôi về mức độ quan trọng của các kết quả khác nhau. Bạn có thể sử dụng dữ liệu thô từ báo cáo này để tự xây dựng danh sách hạng mục đánh giá của riêng mình.

Chi tiết đánh giá Độ chính xác

Về Khả năng bảo vệ

Sản phẩm được thử nghiệm	Tỷ lệ chính xác	Tỷ lệ chính xác (%)
Coro Email and Cloud Security	4,545/4,860	**94%**

Về Khả năng nhận biết tin hợp lệ

Sản phẩm được thử nghiệm	Tỷ lệ chính xác	Tỷ lệ chính xác (%)
Coro Email and Cloud Security	1,070/1,100	**97%**

4. Kết luận

Bài thử nghiệm này đã đặt Coro Email and Cloud Security trước nhiều mối đe dọa khác nhau. Chúng tôi đã sử dụng các phương thức tấn công có mục tiêu đã được ghi nhận trong thực tế, tương tự như cách kẻ tấn công ngoài đời thực áp dụng. Các phương thức này bao gồm Phishing có mục tiêu, mã độc tùy biến, các kỹ thuật xâm nhập doanh nghiệp và các loại hình Social Engineering khác.

Kết quả thử nghiệm cho thấy Coro Email and Cloud Security đã hoạt động hiệu quả trong việc cung cấp lớp bảo vệ bổ sung chống lại các loại hình tấn công email tinh vi thường được triển khai bởi các nhóm tin tặc do quốc gia bảo trợ (APT). Sản phẩm đã phát hiện 99% các cuộc tấn công và có khả năng bảo vệ chống lại 94% trong số đó.

Sản phẩm đã hoạt động rất hiệu quả trong việc nhận biết tin hợp lệ và đạt được Tỷ lệ độ chính xác xuất sắc là 97%. Kết quả này, kết hợp với Tỷ lệ phát hiện chính xác mối đe dọa 99% và Tỷ lệ bảo vệ chính xác 94%, đã góp phần tạo nên Tổng độ chính xác là 94%, một kết quả xuất sắc giúp Coro Email and Cloud Security xứng đáng đem về giải thưởng AAA cho **IPSIP Việt Nam**.

Phụ lục A: Chi tiết các tấn công được sử dụng (1/2)

OilRig (Năng lượng)

Phương thức: Trang web dẫn đến file .exe

Nhóm tấn công bị tình nghi được nhà nước Iran bảo trợ hoạt động từ năm 2014, nhắm vào các lĩnh vực như tài chính, chính phủ và năng lượng thông qua các cuộc tấn công chuỗi cung ứng, sử dụng cơ sở hạ tầng của Iran.

Saint Bear (Chính phủ)

Phương thức: Link ẩn dẫn đến file .exe

Nhóm tấn công threat có liên kết với Nga hoạt động từ năm 2021, nhắm vào Ukraine và Georgia. Nhóm này sử dụng các công cụ như Saint Bot và OutSteel, dựa vào Phishing và các tài liệu giả mạo.

MuddyWater (Quốc phòng)

Phương thức: Link ẩn dẫn đến file .exe

Nhóm gián điệp mạng có liên kết với MOIS của Iran, hoạt động từ năm 2017. Nhóm này nhắm vào các khu vực chính phủ và tư nhân bao gồm quốc phòng, viễn thông và năng lượng trên nhiều châu lục.

Phụ lục A: Chi tiết các tấn công được sử dụng (2/2)

APT38 (Tài chính)

Phương thức: File .exe được nén (.zip)

Nhóm tấn công threat có trụ sở tại Triều Tiên nhắm vào các ngân hàng, tổ chức tài chính và các sàn giao dịch tiền mã hóa tại hơn 30 quốc gia. Các cuộc tấn công đáng chú ý bao gồm Ngân hàng Bangladesh.

APT29 (Nghiên cứu)

Phương thức: shellcode/exe

Có trụ sở tại Nga và có liên kết với cơ quan tình báo nước ngoài. Nhóm này nhắm vào các mạng lưới chính phủ và các viện nghiên cứu bằng cách sử dụng các tệp PDF độc hại đi kèm tài liệu mồi nhử.

Windshift (Hạ tầng trọng yếu)

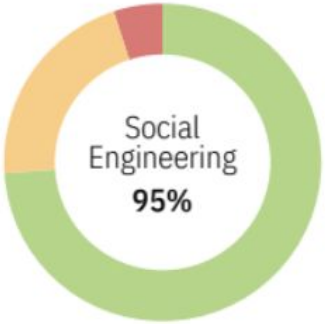
Phương thức: Link ẩn dẫn đến file .exe

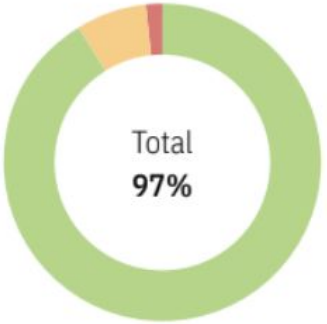
Nhóm tấn công threat hoạt động từ ít nhất năm 2017, nhắm vào các cá nhân cụ thể để giám sát trong các cơ quan chính phủ và cơ sở hạ tầng trọng yếu trên khắp Trung Đông.

Phụ lục B: Hình ảnh trực quan về tấn công có mục tiêu

Targeted Attack Details

Targeted Attack	Stopped	Blocked	Quarantine (admin)	Rejected	Edited (deny)	Quarantine (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	7	0	1	0	2	14	0	0	2
Phishing	34	0	265	0	0	0	1	0	0	0	0
Social Engineering	1	0	73	0	0	0	0	21	0	0	5
Malware	0	0	40	0	20	0	0	0	0	0	0
Total	**35**	**0**	**385**	**0**	**21**	**0**	**3**	**35**	**0**	**0**	**7**





Bảng chi tiết các cuộc tấn công có mục tiêu

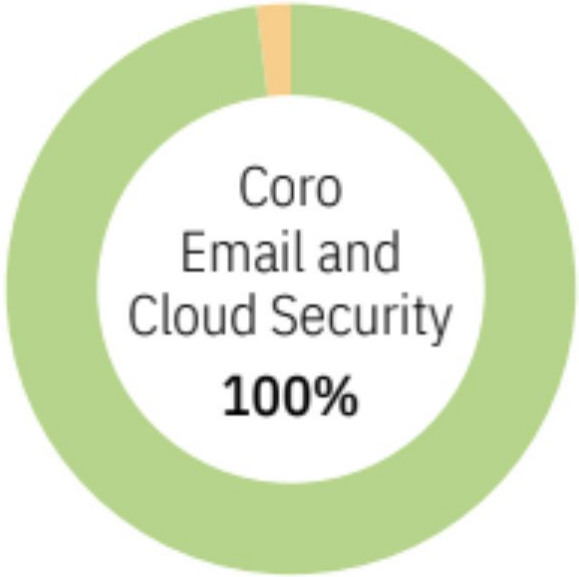
Bảng dưới đây tóm tắt cách sản phẩm dịch vụ xử lý các loại threat phổ biến khác nhau. Sản phẩm được thử nghiệm không nhất thiết phải thực hiện tất cả các phương án xử lý dự kiến, vì vậy bảng chỉ hiển thị những kết quả thực tế đã xảy ra.

Tấn công có mục tiêu	Buộc dừng	Chặn	Thư mục Quarantine (QTV)	Từ chối	Hiệu chỉnh (Từ chối)	Thư mục Quarantine (Người dùng)	Thư mục Junk (Từ chối)	Thư mục Junk	Thư mục Junk (Cho phép)	Hiệu chỉnh (Cho phép)	Hộp thư đến
Business Email Compromise	0	0	7	0	1	0	2	14	0	0	2
Phishing	34	0	265	0	0	0	1	0	0	0	0
Social Engineering	1	0	73	0	0	0	0	21	0	0	5
Malware	0	0	40	0	20	0	0	0	0	0	0
Tổng cộng	35	0	385	0	21	0	3	35	0	0	7

Chi tiết đánh giá Khả năng xử lý tin hợp lệ

Các kết quả này cho thấy mức độ hiệu quả của dịch vụ trong việc xử lý các tin không gây đe dọa. Cân bằng giữa việc cho phép nội dung hợp lệ và chặn nội dung độc hại là yếu tố then chốt đối với hầu hết mọi loại hệ thống bảo mật.

Sản phẩm được thử nghiệm	Hộp thư đến	Hiệu chỉnh (Cho phép)	Thư mục Junk	Thư mục Junk (Cho phép)	Thư mục Quarantine (QTV)	Chặn
Coro Email and Cloud Security	108	0	2	0	0	0



Phụ lục C: Phiên bản sản phẩm

Bảng dưới đây hiển thị tên của sản phẩm dịch vụ được sử dụng trên thị trường tại thời điểm thử nghiệm.

Nhà cung cấp	Sản phẩm	Phiên bản đầu	Phiên bản cuối
Coro	Email and Cloud Security	2.5.65.1 (3.2)	2.5.75.1 (3.4.2)

Phụ lục D: Thuật ngữ (1/2)

Thông báo: Dịch vụ đã ngăn threat được chuyển đến và thông báo cho người dùng. Không có tùy chọn khôi phục.

Buộc dừng: Dịch vụ đã âm thầm ngăn threat được chuyển đến.

Từ chối: Dịch vụ đã ngăn mối đe dọa được chuyển đến và gửi thông báo cho người gửi.

Hiệu chỉnh (Từ chối): Dịch vụ đã chuyển thư đến nhưng chỉnh sửa thư để loại bỏ nội dung độc hại.

Thư mục Junk (Từ chối): Dịch vụ đã chỉnh sửa thư và chuyển thư đến thư mục Junk đích. Nội dung độc hại đã được loại bỏ.

Chặn: Dịch vụ đã ngăn mối đe dọa được chuyển đến và ghi nhật ký sự kiện.

Phụ lục D: Thuật ngữ (2/2)

Thư mục Quarantine (Quản trị viên): Dịch vụ đã ngăn chặn threat được chuyển đến và lưu giữ một bản sao; chỉ quản trị viên mới có thể khôi phục bản sao này.

Thư mục Quarantine (Người dùng): Dịch vụ đã ngăn chặn threat được chuyển đến và lưu giữ một bản sao; người dùng có thể khôi phục bản sao này.

Thư mục Junk: Nền tảng email đã chuyển thư đến thư mục Junk của người dùng.

Thư mục Junk (Cho phép): Dịch vụ đã chỉnh sửa thư và chuyển thư đến thư mục Junk nhưng không loại bỏ nội dung độc hại.

Hộp thư đến: Dịch vụ không phát hiện hoặc không bảo vệ được khỏi threat.

Hiệu chỉnh (Cho phép): Dịch vụ đã chỉnh sửa thư và chuyển thư đến Hộp thư đến đích nhưng không loại bỏ nội dung độc hại.

Phụ lục E: Câu hỏi thường gặp

Tổ chức đối tác là gì? Tôi có thể trở thành đối tác để truy cập dữ liệu về mối đe dọa được sử dụng trong các thử nghiệm của IPSIP không?

Các tổ chức đối tác được hưởng lợi từ dịch vụ tư vấn của chúng tôi sau khi thử nghiệm được thực hiện. Đối tác có thể được truy cập dữ liệu chi tiết, phục vụ các hoạt động cải tiến giải pháp, đồng thời được phép sử dụng logo giải thưởng cho mục đích tiếp thị khi phù hợp. Chúng tôi không chia sẻ dữ liệu cho một bên đối tác thứ ba. Chúng tôi không thiết lập quan hệ đối tác với các tổ chức không tham gia hoạt động thử nghiệm của chúng tôi.

Tôi là nhà cung cấp bảo mật và IPSIP đã thử nghiệm sản phẩm của tôi mà không được phép. Tôi có thể truy cập dữ liệu về mối đe dọa để xác minh tính chính xác của kết quả không?

Chúng tôi sẵn sàng chia sẻ miễn phí một mức dữ liệu thử nghiệm nhất định với các bên tham gia không phải đối tác. Mục đích là cung cấp đủ dữ liệu để chứng minh rằng kết quả là chính xác. Đối với dữ liệu chuyên sâu hơn, phù hợp cho mục đích cải tiến giải pháp, chúng tôi khuyến nghị trở thành đối tác của IPSIP.

Lưu ý về Báo cáo IPSIP Việt Nam

1. Thông tin trong báo cáo này có thể được IPSIP Việt Nam sửa đổi mà không cần thông báo trước.

2. IPSIP Việt Nam không có nghĩa vụ cập nhật báo cáo này vào bất kỳ thời điểm nào.

3. IPSIP Việt Nam tin rằng thông tin trong báo cáo này là chính xác và đáng tin cậy tại thời điểm công bố, nhưng không đưa ra bất kỳ đảm bảo nào về điều này.

4. Nội dung của báo cáo này không cấu thành khuyến nghị, bảo đảm, xác nhận hoặc bất kỳ hình thức chứng thực nào khác đối với các giải pháp được liệt kê, đề cập hoặc thử nghiệm.

5. Quá trình thử nghiệm và các kết quả sau đó không bảo đảm rằng các giải pháp không có rủi ro hoặc bạn sẽ đạt được kết quả tương tự như vậy.

6. Mọi nhãn hiệu, tên thương hiệu, logo hoặc hình ảnh được sử dụng trong báo cáo này đều thuộc về các chủ sở hữu tương ứng.

ipsip VN

Contact us

We're here to help!

ipsip.vn

+84 91 885 30 68

sales-vn@ipsip.eu