시큐리티 라이프싸이클 리뷰

LG CHEM, LTD.

리포트 기간: **17 Days**
시작: Wed, May 18, 2016
종료: Fri, Jun 03, 2016

담당자:
SMARTGATE
Palo Alto Networks

www.paloaltonetworks.com

개요 LG Chem, Ltd.

Key Findings:

- **293** 애플리케이션을 사용 중이며, 이로 인한 잠재적 비즈니스 및 보안 과제가 존재한다. 주요 기능을 조직 관할 외부로 이전하면서 직원들이 업무와 무관한 애플리케이션을 사용하거나 사이버 공격자들이 이를 공격 및 데이터 유출 경로로 사용한다.
- **82** 고위험(high-risk) 애플리케이션이 관찰되었으며, 악성 활동의 침투 또는 은닉에 사용되거나, 네트워크 외부로 파일을 전송하거나, 승인되지 않은 통신을 실행하는 애플리케이션들이 포함되어 있다.
- **1,503,192** 총 위협이 귀사의 네트워크 상에서 발견되었다. 취약성 익스플로잇, 알려진/알려지지 않은 멀웨어, 외부 CnC(command and control) 활동 등이 포함되어 있다.

시큐리티 라이프싸이클 리뷰(Security Lifecycle Review)는 **LG Chem, Ltd.** 의 당면 비즈니스 및 보안 리스크에 대해 요약된 내용을 제공한다. 본 분석에 사용된 데이터는 리포트 해당 기간 동안 팔로알토 네트웍스에 의해 수집되었다. 이 리포트는 애플리케이션, URL 트래픽, 콘텐츠 타입, 네트워크 전반의 위협에 대한 실질적 정보를 제공한다. 아울러 조직의 전반적인 리스크 노출을 줄이기 위한 권고사항을 제공한다.

293
APPLICATIONS IN USE

82
HIGH RISK APPLICATIONS

1,503,192
TOTAL THREATS

1,484,697
VULNERABILITY EXPLOITS

920
KNOWN MALWARE

17,575
UNKNOWN MALWARE

Report Period: 17 Days
Start: Wed, May 18, 2016
End: Fri, Jun 03, 2016

애플리케이션 개요

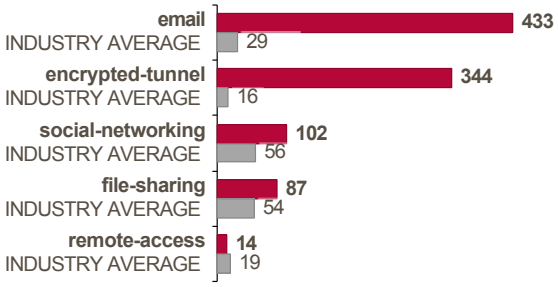
애플리케이션은 위협 경로로 사용되거나, 네트워크 외부로 데이터를 유출시키거나, 승인되지 않은 액세스를 실행하거나, 생산성을 하락시키거나, 기업 대역폭을 소비하는 등의 리스크를 수반할 수 있다. 이 섹션에서는 사용 중인 애플리케이션에 대한 가시성을 제공한다. 이를 토대로 잠재적인 리스크와 비즈니스 이점 사이에서 정확한 정보를 기반으로 현명한 결정을 내릴 수 있다.

주요 조사 결과:

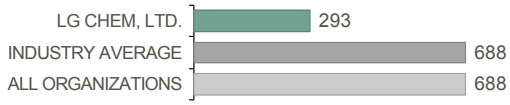
- 네트워크 상에서 **email, encrypted-tunnel 과 social-networking** 등의 고위험 애플리케이션들이 관찰되었다. 악용 가능성이 있는 해당 애플리케이션들에 대한 조사가 실행되어야 한다.
- **28** 개의 하위 카테고리 전반의 네트워크 상에서 총 **293** 개의 애플리케이션이 확인되었다. 다른 **Energy** 조직의 경우 업계 평균적으로 총 **688** 개의 애플리케이션이 확인되었다.
- **general-internet** 의 **1.13TB**를 비롯하여, 총**2.43TB5.19TB**가 전체 애플리케이션들에 의해 사용되었다. 비슷한 조직에서는 업계 평균적으로 **5.19TB**를 사용한다.

고위험 애플리케이션

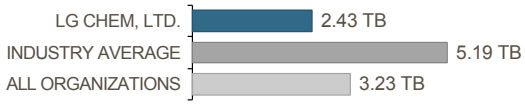
보안 및 비즈니스 리스크 관리의 첫 단계는 어떤 애플리케이션이 악용되어 가장 큰 피해를 초래할 수 있는지 파악하는 것이다. 불필요한 규제, 운영, 사이버보안 리스크를 초래하지 않도록 해당 카테고리의 애플리케이션들을 면밀히 검토할 것을 권장한다.



Number of Applications on Network

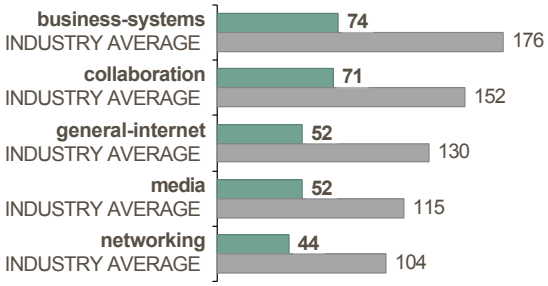


Bandwidth Consumed by Applications



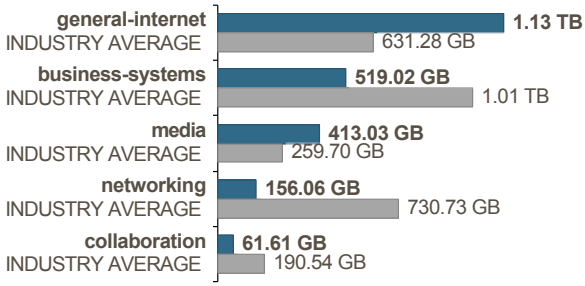
애플리케이션이 가장 많은 카테고리

다음의 카테고리들은 가장 많은 변형 애플리케이션들을 보유하며, 비즈니스 연관성에 대한 검토가 이루어져야 한다.



다음의 카테고리들은 가장 많은 변형 애플리케이션들을 보유하며, 비즈니스 연관성에 대한 검토가 이루어져야 한다.

애플리케이션 카테고리 별 대역폭 소비는 어떤 부분에서 애플리케이션 사용이 가장 많고, 어디서 운영 리소스를 절감할 수 있는지 보여준다.



리스크를 야기하는 애플리케이션

애플리케이션 하위 카테고리 별로 리스크를 야기하는 상위 애플리케이션들(대역폭 소비량 순으로)은 아래와 같다. 다른 **Energy** 조직들의 변종 수에 대한 업계 벤치마크가 포함되어 있다. 이 데이터는 애플리케이션 인에이블먼트(Application Enablement) 작업 시 효과적인 우선순위화를 위해 사용될 수 있다.

RISK LEVEL

5
4
3
2
1

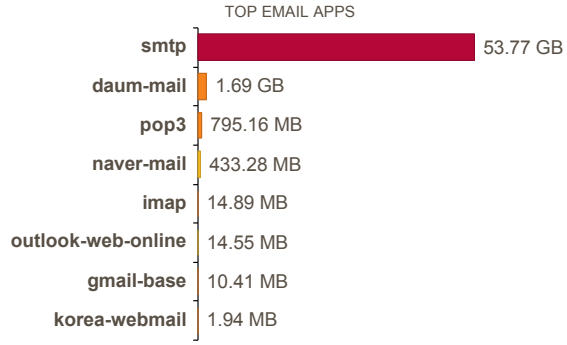
주요 조사 결과:

- 조직 내에서 총 **293** 개의 애플리케이션이 확인되었으며, 다른 **Energy** 조직들의 경우는 업계 평균적으로 **688** 개 이다.
- 애플리케이션 하위 카테고리에서 가장 흔한 유형은 **photo-video, internet-utility 과 file-sharing**이다.
- 가장 많은 대역폭을 소비하는 애플리케이션 하위 카테고리는 **internet-utility, photo-video 과 database**이다.

Email - 56.7GB

14 29

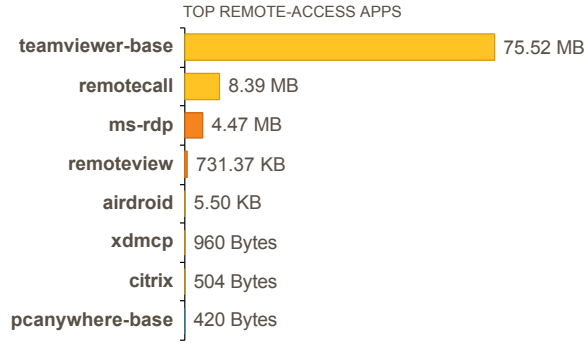
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Remote-Access - 89.09MB

8 19

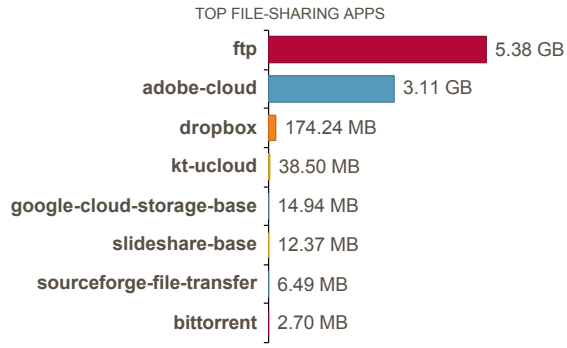
APPLICATION VARIANTS VS INDUSTRY AVERAGE



File-Sharing - 8.73GB

22 54

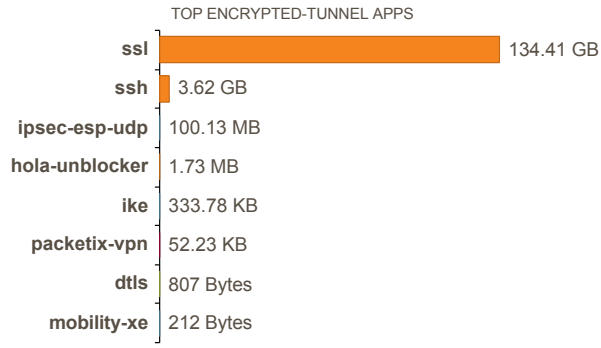
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Encrypted-Tunnel - 138.13GB

8 16

APPLICATION VARIANTS VS INDUSTRY AVERAGE

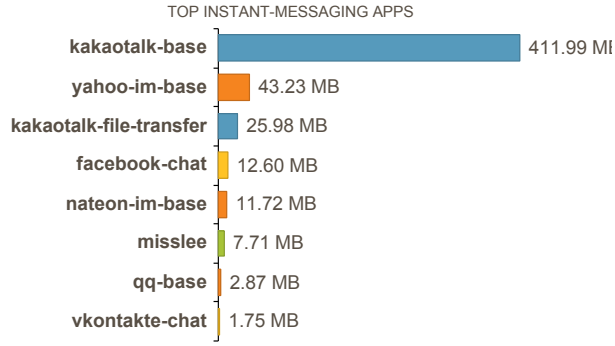


리스크를 야기하는 애플리케이션 (계속)

Instant-Messaging - 522.37MB

18 27

APPLICATION VARIANTS VS INDUSTRY AVERAGE



Social-Networking - 4.24GB

21 56

APPLICATION VARIANTS VS INDUSTRY AVERAGE

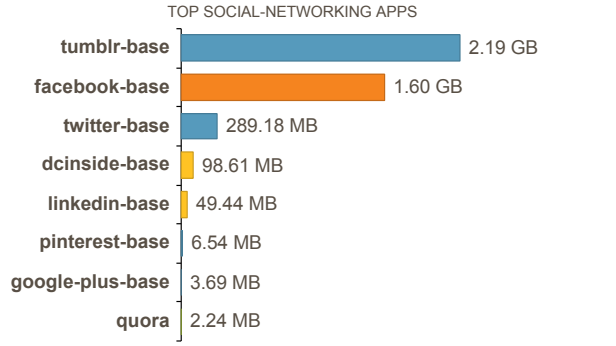
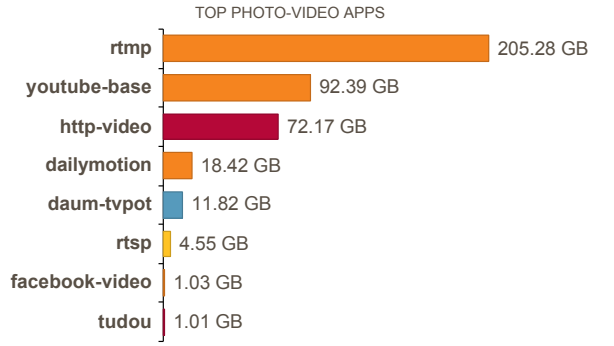


Photo-Video - 409.68GB

38 80

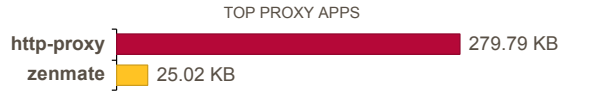
APPLICATION VARIANTS VS INDUSTRY AVERAGE



Proxy - 304.8KB

2 5

APPLICATION VARIANTS VS INDUSTRY AVERAGE



리스크를 야기하는 애플리케이션 — 세부 사항

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
5	smtp	collaboration	email	client-server	53.77GB	204383
4	daum-mail	collaboration	email	browser-based	1.69GB	5501
4	pop3	collaboration	email	client-server	795.16MB	8259
3	naver-mail	collaboration	email	browser-based	433.28MB	17386
4	imap	collaboration	email	client-server	14.89MB	52
3	outlook-web-online	collaboration	email	browser-based	14.55MB	326
4	gmail-base	collaboration	email	browser-based	10.41MB	343
4	korea-webmail	collaboration	email	browser-based	1.94MB	128
4	ssl	networking	encrypted-tunnel	browser-based	134.41GB	94033363
4	ssh	networking	encrypted-tunnel	client-server	3.62GB	36179
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	100.13MB	9
4	hola-unblocker	networking	encrypted-tunnel	client-server	1.73MB	1765
2	ike	networking	encrypted-tunnel	client-server	333.78KB	546
5	packetix-vpn	networking	encrypted-tunnel	client-server	52.23KB	677
1	dtls	networking	encrypted-tunnel	client-server	807Bytes	1
2	mobility-xe	networking	encrypted-tunnel	client-server	212Bytes	2
5	ftp	general-internet	file-sharing	client-server	5.38GB	76717
2	adobe-cloud	general-internet	file-sharing	browser-based	3.11GB	136632
4	dropbox	general-internet	file-sharing	client-server	174.24MB	2354
3	kt-ucloud	general-internet	file-sharing	client-server	38.5MB	5173
2	google-cloud-storage-base	general-internet	file-sharing	browser-based	14.94MB	385
3	slideshare-base	general-internet	file-sharing	browser-based	12.37MB	93
2	sourceforge-file-transfer	general-internet	file-sharing	client-server	6.49MB	1
5	bittorrent	general-internet	file-sharing	peer-to-peer	2.7MB	2431
2	kakaotalk-base	collaboration	instant-messaging	client-server	411.99MB	27036

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
4	yahoo-im-base	collaboration	instant-messaging	client-server	43.23MB	5206
2	kakaotalk-file-transfer	collaboration	instant-messaging	client-server	25.98MB	19
3	facebook-chat	collaboration	instant-messaging	browser-based	12.6MB	219
4	nateon-im-base	collaboration	instant-messaging	client-server	11.72MB	2306
1	misslee	collaboration	instant-messaging	client-server	7.71MB	251
4	qq-base	collaboration	instant-messaging	client-server	2.87MB	4393
3	vkontakte-chat	collaboration	instant-messaging	browser-based	1.75MB	391
4	rtmp	media	photo-video	browser-based	205.28GB	43258102
4	youtube-base	media	photo-video	browser-based	92.39GB	10131
5	http-video	media	photo-video	browser-based	72.17GB	8828
4	dailymotion	media	photo-video	browser-based	18.42GB	662
2	daum-tvpot	media	photo-video	browser-based	11.82GB	38776
3	rtsp	media	photo-video	client-server	4.55GB	23
4	facebook-video	media	photo-video	browser-based	1.03GB	393
5	tudou	media	photo-video	browser-based	1.01GB	2481
5	http-proxy	networking	proxy	browser-based	279.79KB	163
3	zenmate	networking	proxy	browser-based	25.02KB	39
3	teamviewer-base	networking	remote-access	client-server	75.52MB	31
3	remotecall	networking	remote-access	client-server	8.39MB	92
4	ms-rdp	networking	remote-access	client-server	4.47MB	8
4	remoteview	networking	remote-access	client-server	731.37KB	82
3	airdroid	networking	remote-access	browser-based	5.5KB	6
3	xdmcp	networking	remote-access	client-server	960Bytes	16
3	citrix	networking	remote-access	client-server	504Bytes	6
2	pcanywhere-base	networking	remote-access	client-server	420Bytes	7

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	tumblr-base	collaboration	social-networking	browser-based	2.19GB	2377
4	facebook-base	collaboration	social-networking	browser-based	1.6GB	48486
2	twitter-base	collaboration	social-networking	browser-based	289.18MB	11892
3	dcinside-base	collaboration	social-networking	browser-based	98.61MB	2407
3	linkedin-base	collaboration	social-networking	browser-based	49.44MB	1485
2	pinterest-base	collaboration	social-networking	browser-based	6.54MB	512
2	google-plus-base	collaboration	social-networking	browser-based	3.69MB	291
1	quora	collaboration	social-networking	browser-based	2.24MB	6

Notes:

SaaS 애플리케이션

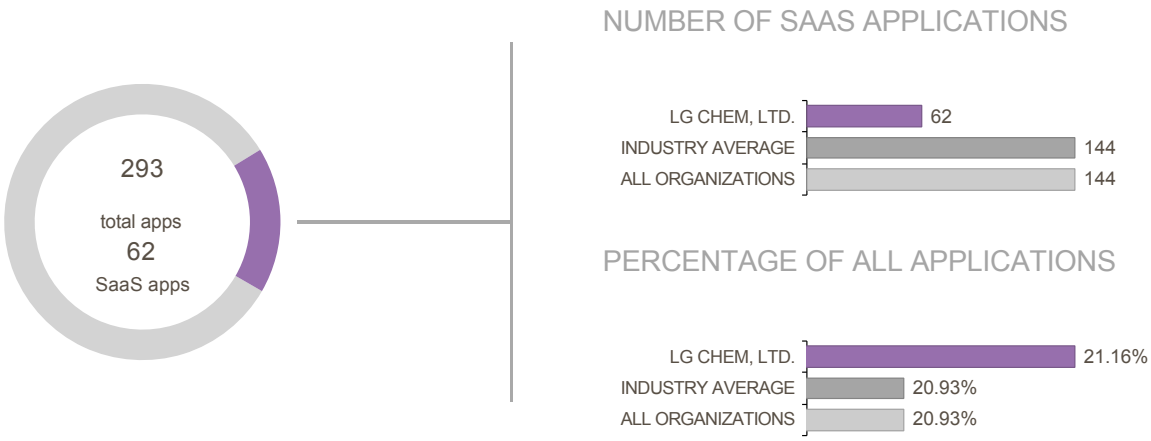
SaaS 기반 애플리케이션 서비스로 인해 네트워크 경계가 모호해지고 있다. 흔히 “Shadow IT”로 표시되는 이러한 서비스의 대부분이 개별 사용자, 사업팀, 또는 부서 전체에 의해 직접 도입된다. 데이터 보안 리스크를 최소화하기 위해서는 SaaS 애플리케이션에 대한 가시성과 적절한 정책이 유지되어야만 한다.

Key Findings

- Your SaaS application usage is more than your industry peers and more than most Palo Alto Networks customers.
- File-sharing subcategory has the most number of unique SaaS applications.
- In terms of data movement, **windows-azure-base** is the most used SaaS application in your organization.

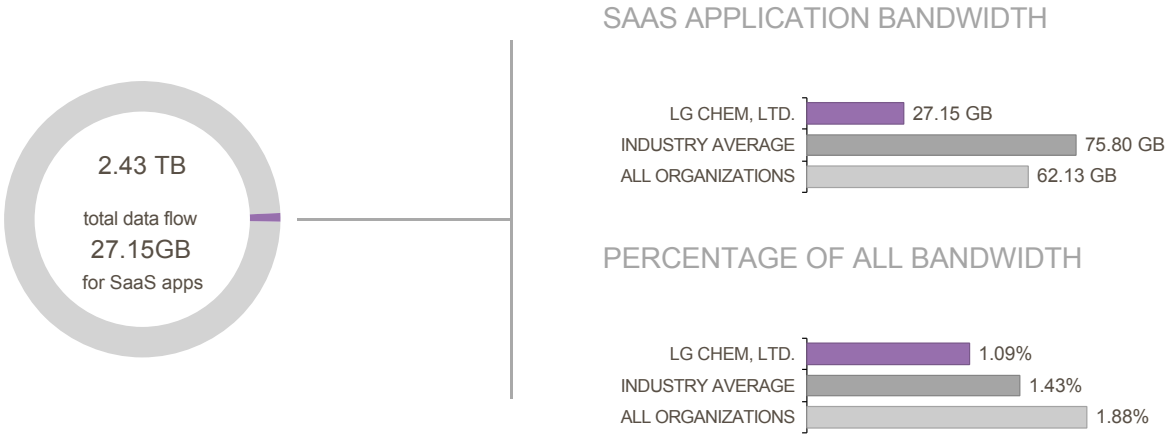
SaaS Applications by Numbers

Review the applications being used in your organization. To maintain administrative control, adopt SaaS applications that will be managed by your IT team



SaaS Application Bandwidth

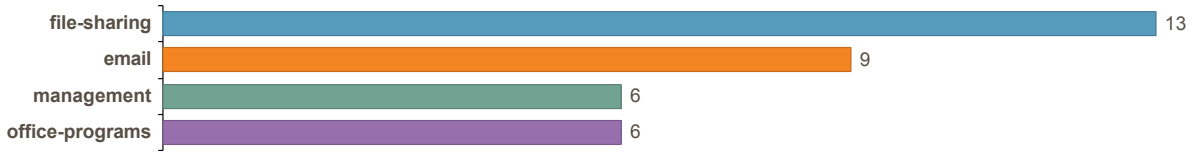
Monitor the volume of data movement to and from SaaS applications. Understand the nature of the applications and how they are being used



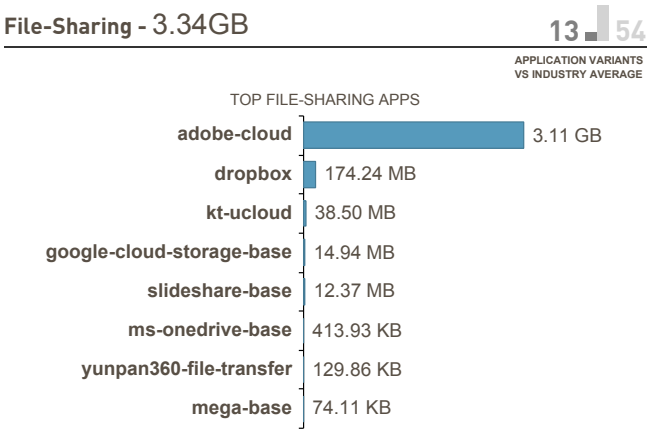
TOP SAAS APPLICATION SUBCATEGORIES

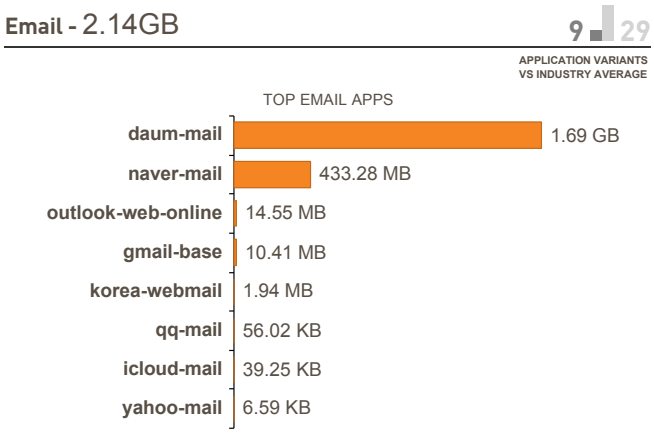
The following displays the number of applications in each application subcategory. This allows you to assess the most used applications organization.

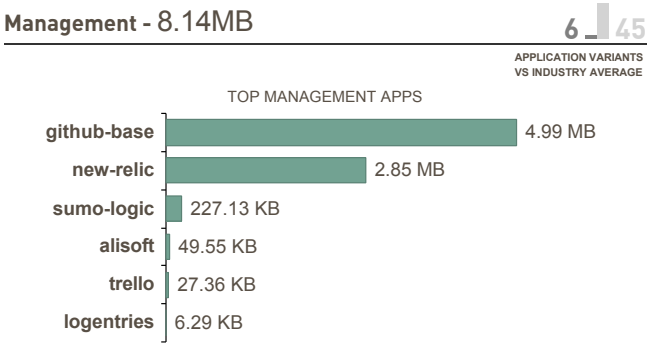
Top SaaS application subcategories by total number of applications

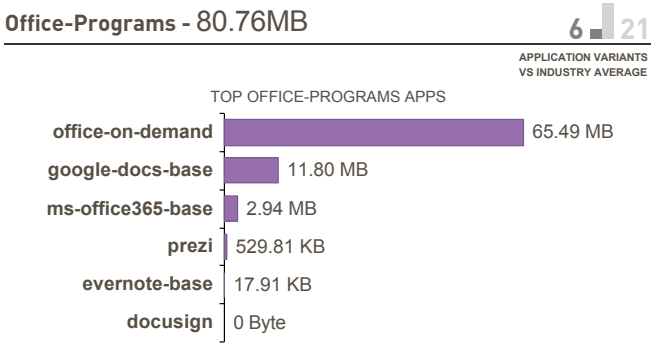


The following shows the top used applications by data movement within the subcategories identified above.





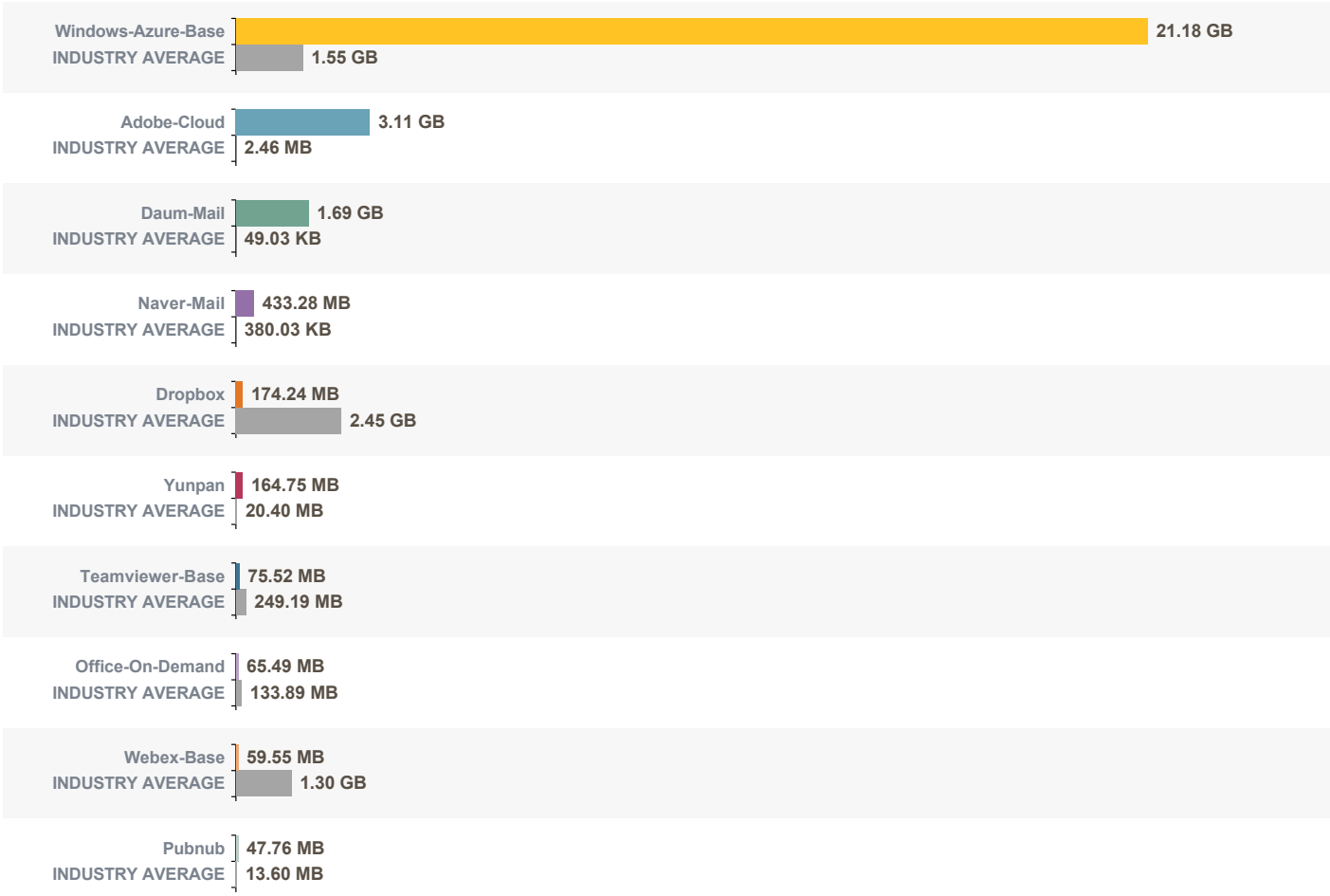




TOP SAAS APPLICATIONS

The following displays the top 10 SaaS applications used in your organization and the application usage comparison against your industry peers and all other Palo Alto Networks customers.

Top SaaS Applications by Data Movement



URL Activity

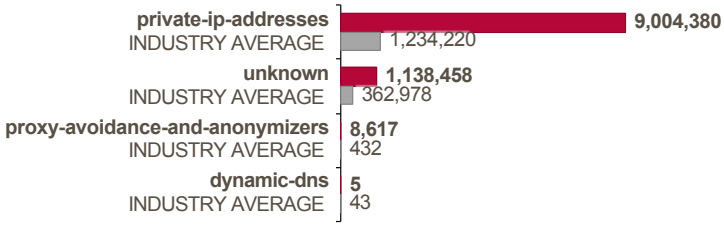
컨트롤되지 않은 웹 서핑으로 인해 조직은 위협 전파, 데이터 유출, 규제 위반 등의 보안 및 비즈니스 리스크에 노출될 수 있다. 네트워크에서 사용자들이 가장 많이 방문한 URL 카테고리는 아래와 같다.

주요 조사 결과:

- 네트워크 상에서 관찰된 고위험 URL 카테고리는 **private-ip-addresses 과 computer-and-internet-info**이다.
- 리포트 해당 기간 동안 사용자들은 **59** 개의 카테고리 전반에서 총 **35,282,229** 개의 URL들을 방문했다.
- 잠재적인 위험성이 있는 웹사이트들을 비롯하여 다양한 개인적, 업무 관련 웹 활동이 이루어졌다.

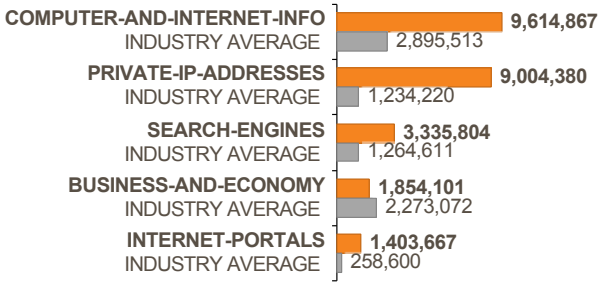
고위험 URL 카테고리

웹은 공격자들이 사용하는 주요 감염 경로이며, 고위험 URL 카테고리는 조직을 막대한 위험에 노출시킨다. 따라서 부적절한 사이트나 악성 사이트를 즉시 차단하고, 알 수 없는 사이트를 신속하게 분류하고 조사할 수 있도록 지원하는 솔루션이 필요하다.



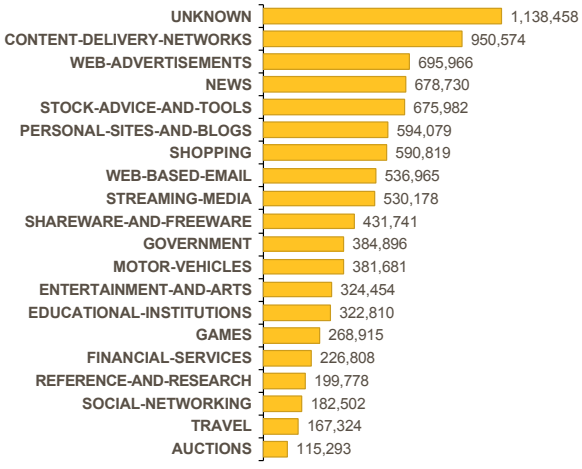
많은 트래픽이 발생하는 URL 카테고리

아래 그림은 사용자들이 많이 방문하는 상위 5개 URL 카테고리와 귀사의 동종 업계 벤치마크를 보여준다.



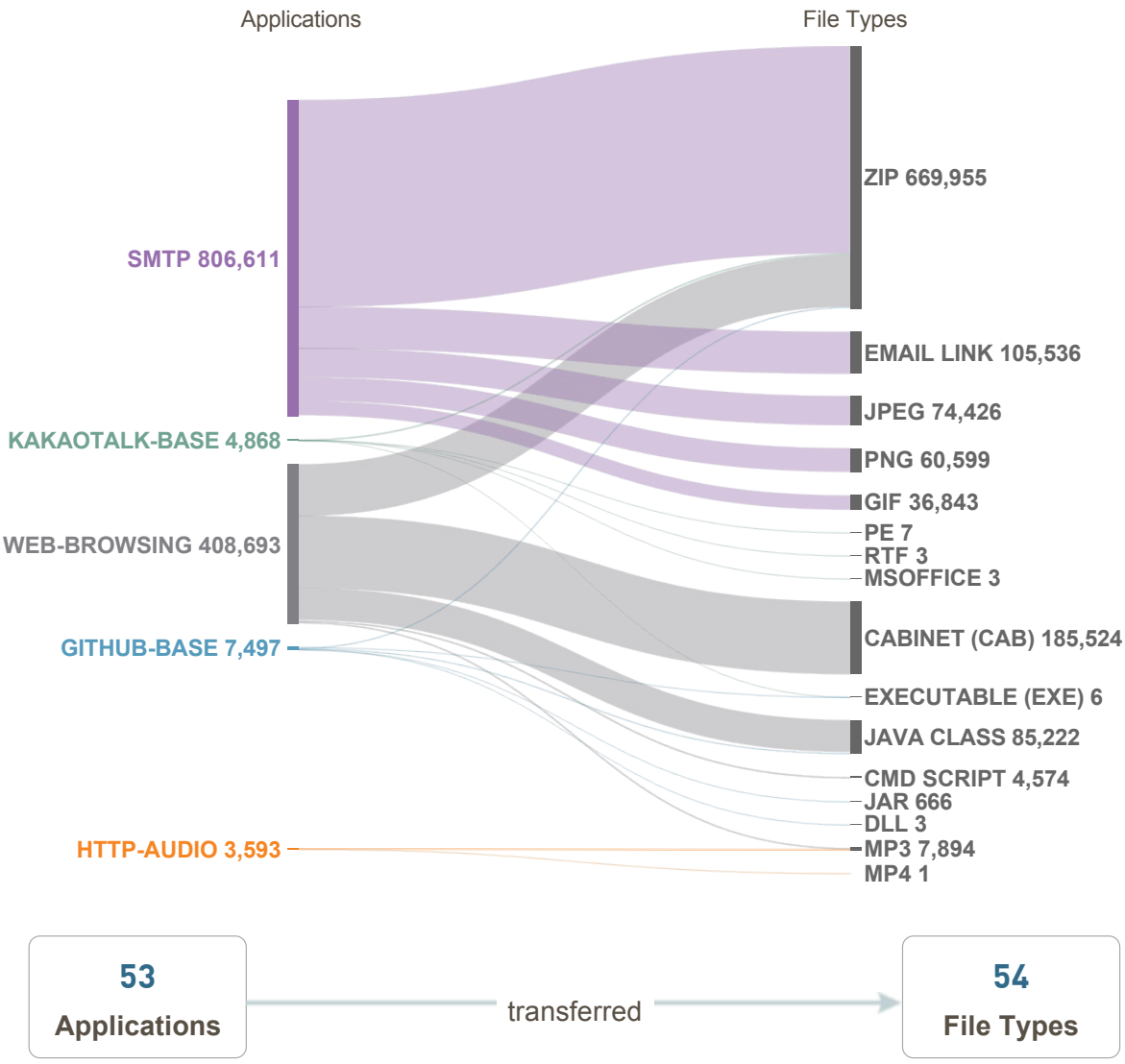
흔히 사용되는 URL 카테고리

사용자들이 가장 많이 방문한 상위 20개 URL 카테고리는 아래와 같다.



파일 전송 분석

파일을 전송할 수 있는 애플리케이션들은 중요한 비즈니스 기능을 수행한다. 그러나 이들은 또한 민감한 데이터를 네트워크 외부로 유출시키거나 사이버 위협의 통로로 이용될 수 있는 가능성이 있다. 귀사의 조직 내에서 총 **53** 개의 애플리케이션을 통해 전송되는**54** 개의 파일 타입의 총 **54** 개의 파일이 관찰되었다. 아래 이미지는 파일 전송에 가장 흔히 사용되는 애플리케이션들과 가장 많이 관찰된 파일 및 콘텐츠 타입을 보여준다.

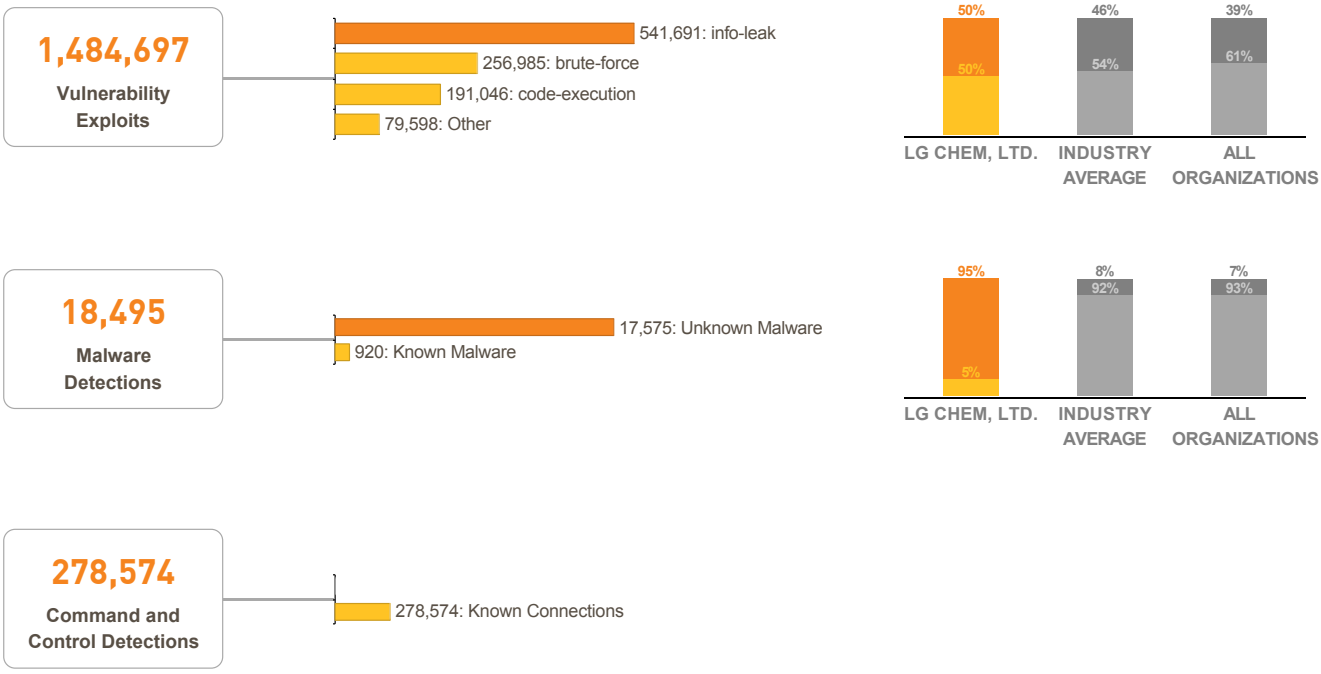


위협 개요

조직의 위협 노출 상태를 파악하고 공격 방지를 위한 보안 태세를 갖추기 위해서는 조직을 노리는 위협의 종류와 양에 대한 인텔리전스가 요구된다. 이 섹션에서는 귀사의 네트워크 상에서 관찰된 애플리케이션 취약성, 알려진/알려지지 않은 멀웨어, CnC(command and control) 활동에 대한 상세 내용을 제공한다.

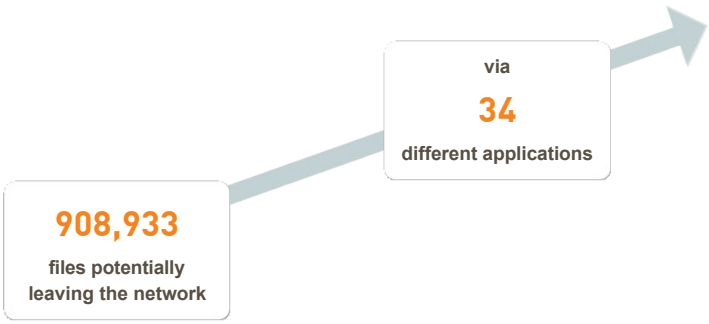
주요 조사 결과:

- 귀사 내에서 총 **1,484,697** 개의 취약성 익스플로잇이 관찰되었으며, 여기에는 **info-leak, brute-force** 과 **code-execution**취약성 카테고리가 포함되어 있다.
- **18,495** 개의 멀웨어 이벤트가 관찰되었으며, 귀사의 동종업계 평균은 **543,632**개이다.
- **278,574** 개의 아웃 바운드 CnC 리퀘스트가 확인되었다. 이것은 멀웨어가 외부 공격자와 통신하여 추가적인 멀웨어 다운로드, 명령 수신, 데이터 유출을 시도했음을 나타낸다.



네트워크 외부로 나간 파일

파일 전송은 업무 수행에 있어서 일반적으로 요구되는 작업이다. 그러나 데이터 유출 위협을 줄이기 위해서는 어떤 콘텐츠가 어떤 애플리케이션을 통해 네트워크 외부로 전송되는지에 대한 가시성을 반드시 유지해야 한다.



고위험 악성 파일 타입 분석

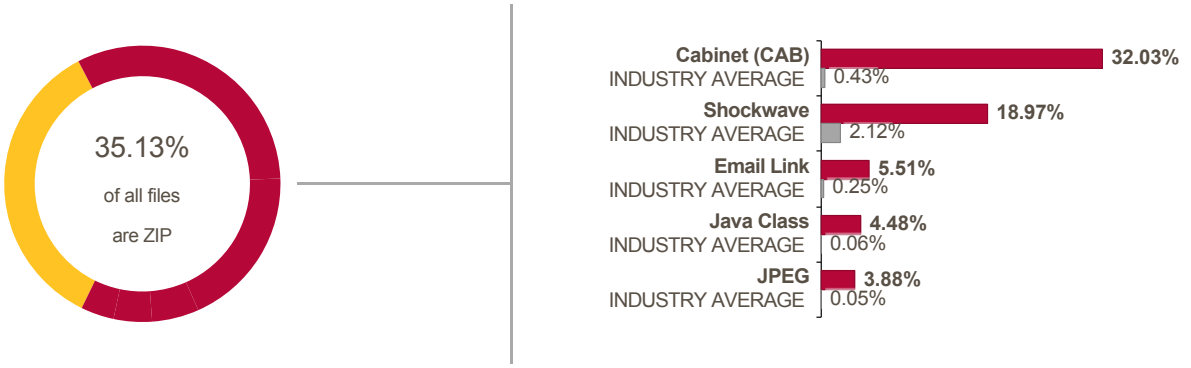
오늘날 사이버 공격자들은 다양한 유형의 파일을 사용하여 멀웨어와 익스플로잇을 전송한다. 대부분의 기업 네트워크에서 사용되는 일반적인 비즈니스 애플리케이션 콘텐츠를 이용하는 경우도 흔하다. 일상적인 애플리케이션에 숨겨진 위협의 대부분이 실행 파일 형태로 전송된다. 이 보다 더욱 타겟화되고 정교한 최신 위협의 경우는 흔히 다른 종류의 콘텐츠를 사용하여 네트워크를 손상시킨다.

주요 조사 결과:

- 다양한 종류의 파일들이 위협을 전송하는데 사용되었다. 방어 전략은 주요 콘텐츠 유형들을 모두 커버해야 한다.
- 인터넷에서 실행 파일 다운로드를 차단하거나 일상적인 업무와 무관한 RTF 파일 또는 LNK 파일을 불허하는 등, 고위험 파일 타입을 선제적으로 차단함으로써 조직에 노출되어 있는 공격 경로를 줄일 수 있다.

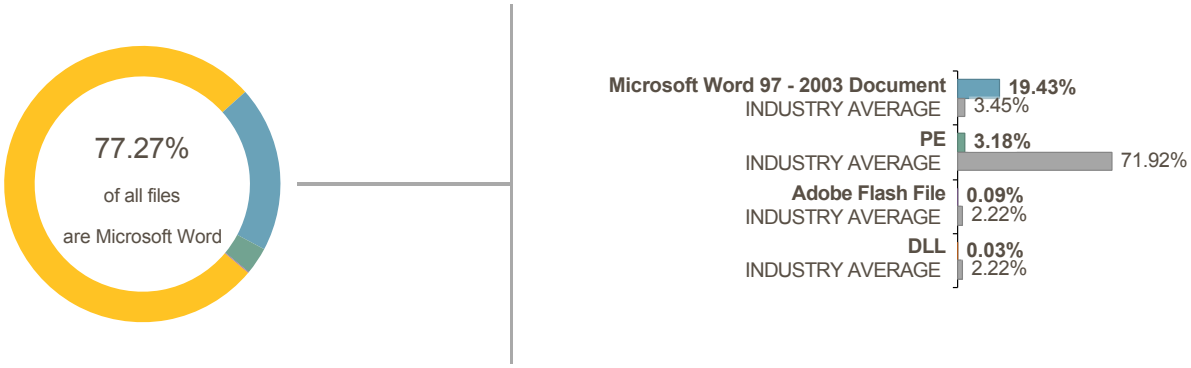
고위험 파일 타입

그림에 나와 있는 파일 타입들은 패치 되지 않은 기존 결함 외에도 새로운 취약성들이 발견되고 있고, 공격에 자주 사용되는 까닭에 고위험군으로 분류된다.



알려 지지 않은 멀웨어를 운반하는 파일

조직 내부 및 외부로 위협을 전파하는데 사용될 수 있는 파일들을 조사할 것을 권장한다. 이와 함께 서로 다른 사용자 그룹 간에 고위험 파일 타입의 전송을 차단하는 등 예방 조치를 취하도록 한다.

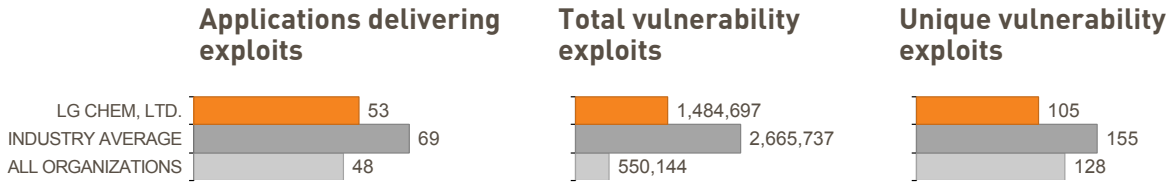


애플리케이션 취약성

공격자들은 애플리케이션 취약성을 악용하여 취약하고 패치되지 않은 애플리케이션을 익스플로잇(exploit)하고 시스템을 감염시킨다. 이와 같은 애플리케이션 취약성 익스플로잇이 흔히 보안 침해의 첫 단계로 나타난다. 이 페이지에서는 귀사 내에서 공격자들이 가장 빈번하게 익스플로잇을 시도한 상위 5개 애플리케이션 취약성에 대해 설명한다. 이를 통해 귀하는 어떤 애플리케이션이 가장 많은 공격 경로를 수반하는지 확인할 수 있다.

주요 조사 결과:

- **53** 개의 애플리케이션이 귀사의 환경에 익스플로잇을 들여오는 것으로 관찰되었다.
- **1,484,697** 개의 취약성 익스플로잇이 관찰되었으며, 가장 많은 상위 3개 카테고리는 **web-browsing, smtp 과 ssh**이다.
- 발견된 전체 취약성 중에서, **105**개의 고유한 취약성이 발견되었다. 이는 공격자들이 동일한 취약성 익스플로잇을 반복적으로 사용했음을 의미한다.



Vulnerability Exploits per Application (top 5 applications with most detections)

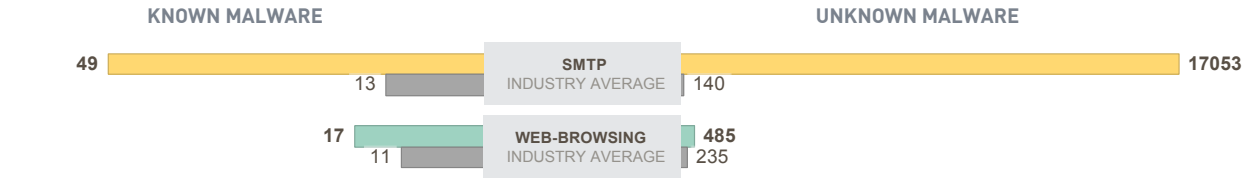
DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
648,052	**web-browsing**			
16	Microsoft Lync Server Information Disclosure Vulnerability	Critical	code-execution	CVE-2014-1823
9	RIG Exploit Kit Detection	Critical	exploit-kit	
3	jQuery.min.php Redirect Detected	Critical	code-execution	
1	MAGNITUDE Exploit Kit Detection	Critical	code-execution	
3	ANGLER Exploit Kit Detection	Critical	code-execution	
4	PHP CGI Query String Parameter Handling Code Injection Vulnerability	High	code-execution	CVE-2012-1823;CVE-2012-2311
208,241	**smtp**			
4,730	MAIL: User Login Brute-force Attempt	High	brute-force	
29	JavaScript Obfuscation Detected	Medium	code-execution	
1	Postfix SMTP Service STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	Medium	code-execution	CVE-2011-0411
183,362	Javascript Sent in Email	Info	code-execution	
13,918	Failed Authentication Through Mail Protocol	Info	brute-force	
6,138	Adobe PDF File With Embedded Javascript	Info	code-execution	CVE-2008-0655;CVE-2007-5659;CVE-2007-5663;CVE-2007-5666;CVE-2008-0667;CVE-2008-0726;CVE-2008-2042
43,018	**ssh**			
43,018	SSH2 Login Attempt	Info	brute-force	
23,726	**eset-remote-admin**			
11,870	HTTP WWW-Authentication Failed	Info	brute-force	
11,856	HTTP Unauthorized Error	Info	brute-force	
23,499	**ftp**			
5,883	FTP: login Brute-force attempt	High	brute-force	
17,616	FTP Login Failed	Info	brute-force	

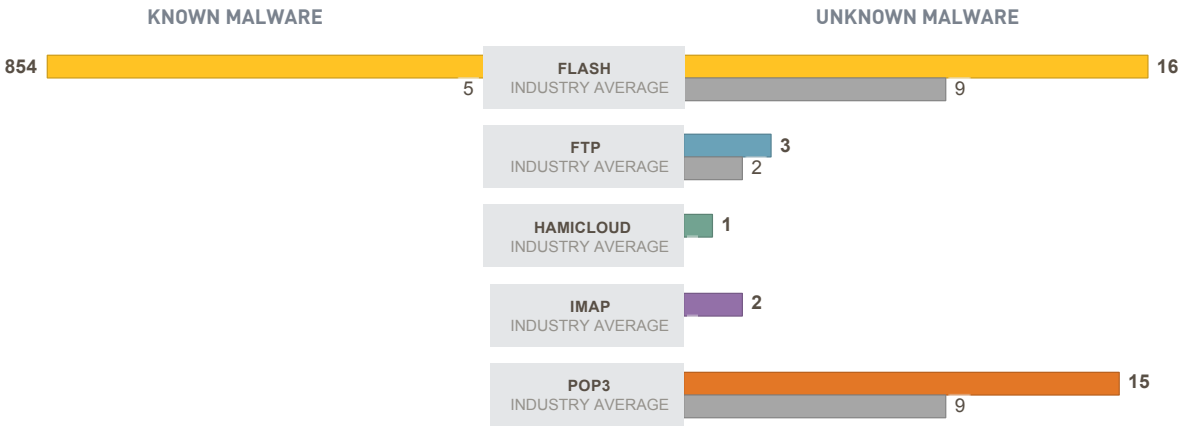
알려진/알려지지 않은 멀웨어

애플리케이션은 공격자가 멀웨어를 전송하고, 조직을 감염시키는고, 외부 CnC 서버와 통신하고, 데이터를 유출시키는데 흔히 사용되는 주요 경로이다. 공격자의 전술이 갈수록 진화하여 이제는 전통적인 보안 솔루션들이 거의 확인하지 못하는 네트워크 상의 일반적인 애플리케이션을 사용하는 단계에 이르렀다.

주요 조사 결과:

- 네트워크 상의 총 **293** 개의 애플리케이션 중 **7** 개의 애플리케이션이 귀사 조직 내에서 멀웨어를 옮기고 있는 것으로 관찰되었다.
- 멀웨어를 전달하는 애플리케이션들 가운데 상당수가 업무 수행에 꼭 필요한 애플리케이션들이다. 따라서 귀사는 이러한 애플리케이션들을 지원하는 동시에 위협을 방지할 수 있는 솔루션이 필요하다.
- 대부분의 멀웨어가 HTTP 또는 SMTP를 통해 전송된다. 최신 공격은 흔히 비표준 포트나 다른 우회 기법을 채용한 다른 애플리케이션들을 사용한다.





7
applications found delivering malware

CnC(Command and Control) 분석

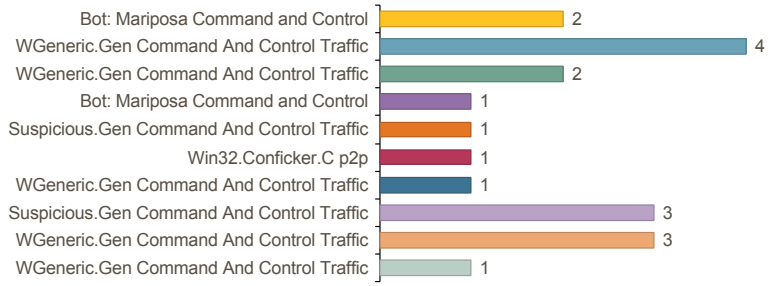
CnC(Command-and-control) 활동은 네트워크 내 호스트가 멀웨어에 감염되어 네트워크 외부의 공격자와 연결을 시도하고 있음을 나타낸다. 공격자가 CnC를 사용하여 추가적인 멀웨어를 침투시키고 명령을 내리거나 데이터를 유출시키므로 이러한 활동을 이해하고 방지하는 것이 매우 중요하다.

주요 조사 결과:

- **4** 개의 애플리케이션이 CnC 커뮤니케이션에 사용되었다.
- 귀사의 네트워크로부터 총 **278,574** 개의 CnC 리퀘스트가 관찰되었다.
- 총 **46,626** 건의 의심스러운 DNS 쿼리가 관찰되었다.

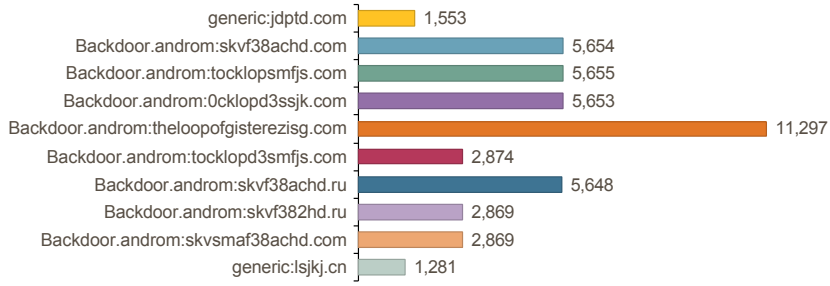
스파이웨어 폰 홈(Phone Home) 231,948

아래 이미지는 외부 악성 CnC 서버와의 연결을 시도하는 감염된 호스트를 나타낸다.



의심스러운 DNS 쿼리 46,626

DNS는 일반적이고 필요한 애플리케이션이지만, 아래 차트에 나온 것과 같이 아웃바운드 CnC 커뮤니케이션을 숨기는 데에도 흔히 사용된다.



요약 LG Chem, Ltd.

본 분석을 통해 네트워크 상에 존재하는 다양한 애플리케이션과 사이버공격을 확인하였다. 이번 작업은 **LG Chem, Ltd.**의 잠재적인 비즈니스 및 보안 리스크를 파악하는 동시에, 지속적인 비즈니스 성장과 조직 전반의 리스크 노출을 줄이는 "세이프 애플리케이션 인에이블먼트(Safe Application Enablement)" 정책 실행을 위한 이상적인 기회가 될 것이다.

하이라이트:

- 네트워크 상에서**email, encrypted-tunnel 과 social-networking** 등의 고위험 애플리케이션들이 관찰되었다. 악용 가능성이 있는 해당 애플리케이션들에 대한 조사가 실행되어야 한다.
- **28** 개 전반의 네트워크 상에서 총 **293** 개의 애플리케이션이 확인되었다. 다른 **Energy** 조직의 경우 업계 평균적으로 총 **688** 개의 애플리케이션이 확인되었다.
- **1,484,697** 개의 취약성 익스플로잇이 관찰되었으며, 가장 많은 상위 3개 카테고리는 **web-browsing, smtp 과 ssh**이다.
- **18,495** 개의 멀웨어 이벤트가 관찰되었으며, 귀사의 동종업계 평균은 **543,632** 개 이다.
- **4** 개의 애플리케이션이 CnC 커뮤니케이션에 사용되었다.

293
APPLICATIONS IN USE

82
HIGH RISK APPLICATIONS

1,503,192
TOTAL THREATS

1,484,697
VULNERABILITY EXPLOITS

920
KNOWN MALWARE

17,575
UNKNOWN MALWARE

권고 사항:

- 업무에 필요한 애플리케이션만 허용하고 다른 모든 애플리케이션들에 대해정교한 컨트롤을 적용하는 "세이프 애플리케이션 인에이블먼트(Safe Application Enablement)" 정책을 실행할 것.
- 리모트 액세스, 파일 공유, 암호화 터널 등 침해 가능성이 있는 고위험애플리케이션들에 대한 대응 솔루션을 마련할 것.
  알려진/알려지지 않은 위협을 모두 탐지하고 방어하여 공격자로부터의리스크를 완화시킬 수 있는 보안 솔루션을 구축할 것.
- 스스로 자동 재프로그래밍을 실행하고, 최신 위협에 대한 새로운 보호를생성하고, 전세계 기업 사용자 커뮤니티로부터 최신 정보를 업데이트하는솔루션을 사용할 것.