



Leaking Beeps: A Closer Look at IT Systems That Leak Pages

Stephen Hilt and Philippe Lin
Trend Micro Forward Looking Threat Research

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

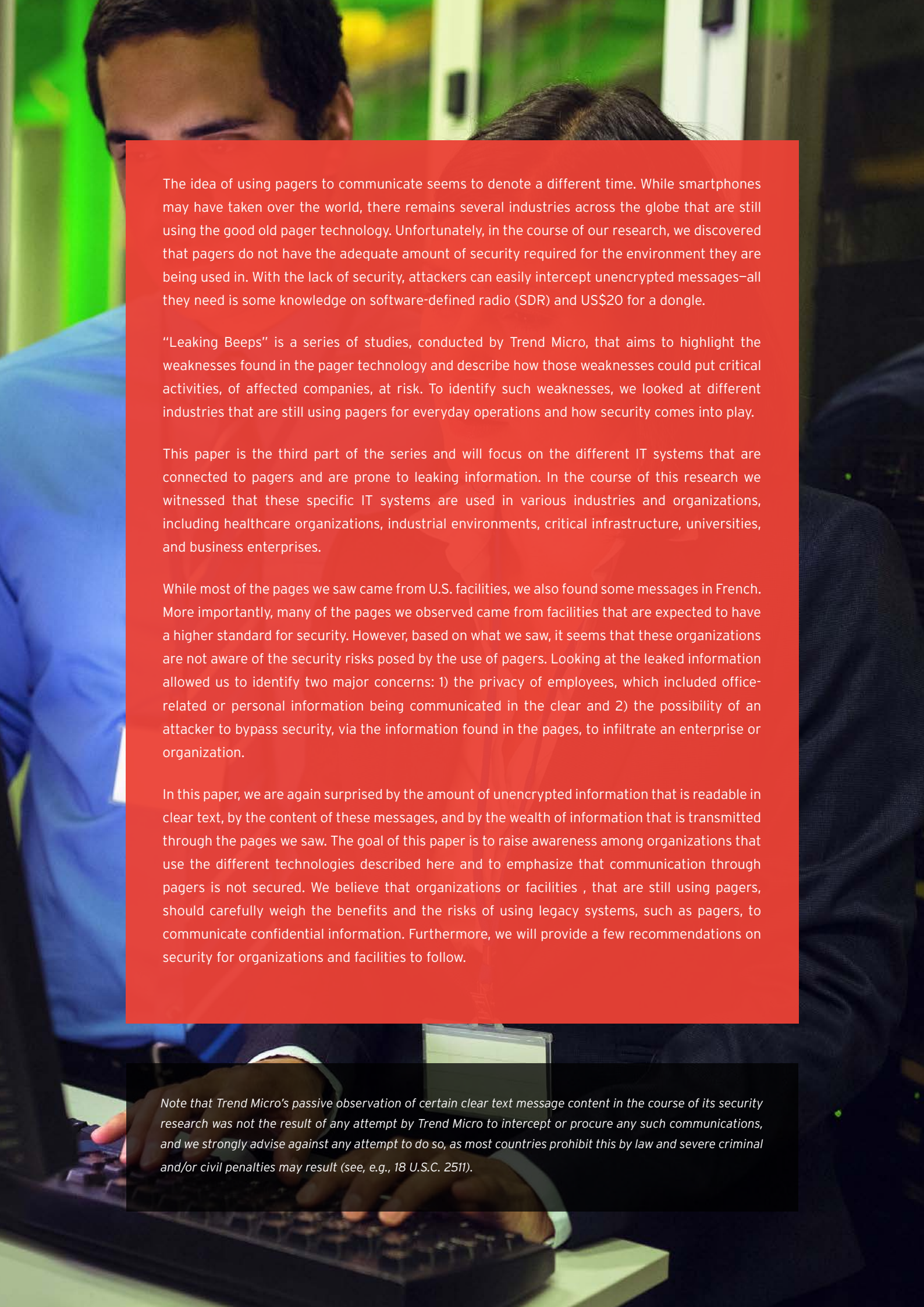
Leaked Information and
the Potential for Damage

14

Possible Attack Scenarios
and How Leaked Pages
can be Misused

22

Conclusion



The idea of using pagers to communicate seems to denote a different time. While smartphones may have taken over the world, there remains several industries across the globe that are still using the good old pager technology. Unfortunately, in the course of our research, we discovered that pagers do not have the adequate amount of security required for the environment they are being used in. With the lack of security, attackers can easily intercept unencrypted messages—all they need is some knowledge on software-defined radio (SDR) and US\$20 for a dongle.

“Leaking Beeps” is a series of studies, conducted by Trend Micro, that aims to highlight the weaknesses found in the pager technology and describe how those weaknesses could put critical activities, of affected companies, at risk. To identify such weaknesses, we looked at different industries that are still using pagers for everyday operations and how security comes into play.

This paper is the third part of the series and will focus on the different IT systems that are connected to pagers and are prone to leaking information. In the course of this research we witnessed that these specific IT systems are used in various industries and organizations, including healthcare organizations, industrial environments, critical infrastructure, universities, and business enterprises.

While most of the pages we saw came from U.S. facilities, we also found some messages in French. More importantly, many of the pages we observed came from facilities that are expected to have a higher standard for security. However, based on what we saw, it seems that these organizations are not aware of the security risks posed by the use of pagers. Looking at the leaked information allowed us to identify two major concerns: 1) the privacy of employees, which included office-related or personal information being communicated in the clear and 2) the possibility of an attacker to bypass security, via the information found in the pages, to infiltrate an enterprise or organization.

In this paper, we are again surprised by the amount of unencrypted information that is readable in clear text, by the content of these messages, and by the wealth of information that is transmitted through the pages we saw. The goal of this paper is to raise awareness among organizations that use the different technologies described here and to emphasize that communication through pagers is not secured. We believe that organizations or facilities , that are still using pagers, should carefully weigh the benefits and the risks of using legacy systems, such as pagers, to communicate confidential information. Furthermore, we will provide a few recommendations on security for organizations and facilities to follow.

Note that Trend Micro's passive observation of certain clear text message content in the course of its security research was not the result of any attempt by Trend Micro to intercept or procure any such communications, and we strongly advise against any attempt to do so, as most countries prohibit this by law and severe criminal and/or civil penalties may result (see, e.g., 18 U.S.C. 2511).

Leaked Information and the Potential for Damage

Across various organizational settings, there are multiple tools that are being used in combination with pagers. Unfortunately, these IT technologies inadvertently have a lot of potential for leaking information. In this section we will take a look at the different tools used together with pagers, such as SMS-to-pager and email-to-pager gateways. At the same time, we will also show examples of sensitive information that were leaked through the use of pagers.

SMS-to-Pager Gateway

SMS-to-pager gateways have a specific set of phone numbers, which receive the SMS that will be forwarded to a pre-configured pager. It is also very similar to the email-to-pager gateways we discussed in the previous paper. The only difference is that instead of a special email address, the page comes with the prefix SMS:[phone-number]. We saw SMS-to-pager gateways widely used to send personal messages, by 911, the healthcare sector, some industrial control systems (ICS), and a system that logs missed calls. The messages below are modeled after what we saw:

```
911 - Fr:SMS:[NUMBER].CCD:ASSAULT!_R SEXUAL ASSAULT HA;280 [STREET NAME];MAUL;MILLER
RD;SHADECREST DR;(S) (N)60A;MAULDIN FIRE IS ENROUTE[05/16/16 10:59:19 MMITCHELL] Mauldin
PD on sc
```

```
Healthcare -Fr:SMS:[NUMBER].Please call 3936. Heart cath for Ted patient in
[ORGANIZATION]. Dr [NAME].
```

```
ICS -Fr:SMS:[NUMBER].-- OmniSite Notification - .[ORGANIZATION] has a High Wet Well Level
Alarm Condition at 9:21 AM on 4/25/2016.Call [PHONE NUMBER] to acknowledge. [66]
```

```
Personal messages -Fr:SMS:[NUMBER]. Also, don't forget rehearsal tonight. Love you. [49]
```

```
Spams - Fr:SMS:[NUMBER].NEW XXX Ladies - LIVE DJ -. Pvt Lap Dance rooms - Bar Specials  
- Inv by Ms WEBB - for exact addr text me 'Wet WED' ---- THU Apr 7th XXX [ORGANIZATION]  
[58]
```

```
Missed calls -Fr:SMS:[NUMBER].Missed call on cell from [NAME] [NUMBER] via Android [16]
```

By looking at the pages sent through SMS-to-pager gateways, it was easy to determine who sent the SMS and in what particular industry the sender is involved in. In the months we observed leaked pages, we were able to establish a pattern of communication between a fixed pair of communicators. For example one of the pages, containing the message “Call Me”, supported the idea that there are some communicators that already have established ties with others—meaning both parties have a clear idea of who the sender is even without a proper introduction from the sender.

| | |
|------------|----------------------------------|
| 2016-02-23 | Fr:SMS: [PHONE NUMBER1]. Call me |
| 2016-02-24 | Fr:SMS: [PHONE NUMBER2].Call me |
| 2016-03-31 | Fr:SMS: [PHONE NUMBER3].Call me |
| 2016-04-25 | Fr:SMS: [PHONE NUMBER4].Call me |
| 2016-05-05 | Fr:SMS: [PHONE NUMBER5] Call me |
| 2016-05-09 | Fr:SMS: [PHONE NUMBER6].Call me |

CallXPress

One organization we observed was seen using CallXpress¹ along with a speech-to-text voicemail summary system that we could not identify. CallXpress is a commercial service that provides unified messaging to email systems (Microsoft® Outlook®, Lotus Notes®, etc.) as well as voicemail and fax. Users can access those messages from a cellphone, a web interface, and even a telephone. CallXpress also provides a voicemail transcription service and a phonebook service to its clients. In the following sections, we will discuss how a phonebook can be used by malicious actors to compromise a target's privacy.

SPOK®

Spok Inc., formerly known as USA Mobility, is a provider of critical communication solutions that was formed after Amcom Software and USA Mobility Wireless merged.² According to Spok's website, the service targets clinical alerting and notifications, hospital communications, wide-area paging, emergency

communication, and 911 call center solutions, etc. They provide regular service as well as an encrypted paging service called “T5”. Since cracking encrypted communication was not among the goals of our research (and would also be illegal in most jurisdictions), we focused on observing unencrypted messages only.

We saw messages that mentioned Spok. Those messages looked similar to this:

```
You are needed on the Spok conf. call [PHONE NUMBER] Access Code: [CODE NUMBER]
```

We also saw messages from the old company name, usamobility.net and notifyatonce.net:

```
From: CC_Message_Notification@usamobility .net - [EMAIL ADDRESS]: [NAME], could  
you please give me a call when you receive this page? [NAME] [PHONE NUMBER]
```

```
From: [EMAIL ADDRESS]@notifyatonce .net - WTI: Today, 13:30, 9723/14 CR, Re:  
Machinist Hand Injury. POC, [NAME], [PHONE NUMBER]
```

A system that looks up CallerID

In the first paper of the series, we talked about Health Insurance Portability and Accountability Act (HIPAA) violations. Based on our findings, a system that looks up CallerID in the phonebook can leak a lot of information and thereby constitute a violation of privacy regulations. We found that the CallerID function of this system exposed 135 patients’ names, phone numbers, pregnancy statuses, birthdates, as well as information on illnesses and symptoms. The researchers, however, were unable to recognize the system’s name.

```
Fr:SMS:[NUMBER].Caller: [NAME] [PHONE NUMBER]; Caller is Patient: Yes Status:  
Non Pregnancy Matter DOB: 12/06/1960 acid reflux causing bad coughing at night,  
got - (p1/2)
```

```
Fr:SMS:[NUMBER].Caller: [NAME] [PHONE NUMBER] ; Caller is Patient: Yes Status:  
Non Pregnancy Matter DOB: 01/10/1980 Hasnt had bowell movement since last thurs  
- (p1/2)
```

```
Fr:SMS:[NUMBER].Caller: [NAME][PHONE NUMBER]; Caller is Patient: Yes Status:  
Non Pregnancy Matter DOB: 03/05/1953 Been sick 3 days fell 3 times Emerg: Yes  
-(p1/2)
```

SNMP

A SNMP (Simple Network Management Protocol) alert or trap message, which is sent to operation engineers, can be very useful when they are in a facility that prohibits cellphone usage or when they simply do not have a company phone. In the alerts we observed, however, we could see intranet hostnames, IP, and trap messages that to some point reveal information on problems with the server. The messages below are similar to what we saw:

```
Fr:SMS:[NUMBER].ALERT: pdb-warehouse (xx.x.x.22) my status/my slave lag (SNMP  
Library) Down ESCALATION REPEAT No such instance (SNMP error # 223)
```

```
Fr:SMS:[NUMBER].ALERT: app-01 ( xx.x.xx.51 ) Load Avg. (SNMP Linux Load Average)  
Threshold reached (1 Minute) (12 ) 114 (1 Minute) is above the error limit of  
25
```

```
Fr:SMS:[NUMBER].(I.T. Monitoring) 5 Summarized Notifications (5 Down) https://  
eyes.telcentris.net/
```

Email-to-Pager Gateway

Similar to the SMS-to-pager gateways, another similar type of service available is the email-to-pager gateway. An email-to-pager gateway is a service, usually provided by a third party company, that forwards emails sent to a specific address to predefined paging numbers. In the second paper in the series, we discussed how email-to-pager gateways leaked information in, but not limited to, industrial control systems. In this section, we will describe the various attack surfaces that malicious actors can use through email-to-pager gateways.

WhosCalling®

WhosCalling is a system that sends an email to people who missed calls. During our research, we saw about 3,000 WhosCalling records from a single facility. At first glance, the data does not look problematic

nor does it look like it is revealing too much information about the users. However, people with bad intentions could easily collect this type of data to compile a comprehensive phonebook, which they can use for future attacks.

```
From: [EMAIL ADDRESS] Subject: WhosCalling - 01/:8 09:53 [PHONE NUMBER 1] [NAME 1]
```

```
From: [EMAIL ADDRESS] Subject: WhosCalling - 01/28 09:59 [PHONE NUMBER 2] [NAME 2]
```

```
From: [EMAIL ADDRESS] Subject: WhosCalling - 01/28 10:00 [PHONE NUMBER 3] [NAME 3]
```

WhatsUp® Gold, ARSystem, Nagios®

Ipswitch's WhatsUp Gold is a server and network monitoring solution.³ Similar to the SNMP trap sent via a SMS-to-pager gateway, one can collect intranet intelligence in an organization via these tools. For example, we could identify servers (namely LDAP servers) where authentication and account information are stored in an organization. The information on LDAP servers and private IPs, which provide an overview of the intranet topology, can aid hackers who have already penetrated a company and want to move laterally.

- C2k[HOSTNAME] (10.xx.x.44)
- C2k[HOSTNAME] (10.xx.xx.2)
- C2k[HOSTNAME] (10.xx.x.104)
- ldap (10.xx.xx.28)
- ldap (10.xx.xx.31)
- ldap (10.xx.xx.33)
- ldap (10.xx.x.24)
- ldap (10.xx.xx.2)
- ldap (10.xx.x.28)

During our research, the messages on WhatsUp Gold helped us identify which router models were experiencing a downtime. With this type of information, (e.g. downtime and model of routers), an attacker can get inside an organization by exploiting specific vulnerabilities found in those routers.


```
WCP-Sxxxxxx (Cisco cisco1941 Router) is Down at least 20 min(172.19.x.xx). -  
Interface(10) Internal Interface (172.16.x.xx)
```

```
MPLS WCP-Sxxxxxx CE S0/0/0 (Router) is Down at least 20 min(xxx.xx.x.182)
```

```
WCP-Kxxxxxxx (Cisco cisco1841 Router) is Down at least 20 min(172.19.x.xx)
```

```
WCP-Rxxxxxx (Cisco cisco1941 Router) is Down at least 20 min(172.19.x.xx)
```

```
WCP-WH2-xxxxxxx (Cisco Router) is Down at least 20 min(172.16.x.xx)
```

```
WCPxxxx.CAS (Windows 2008 Server) is Down at least 20 min(172.16.x.xx)
```

Meanwhile, Nagios is a widely used monitoring system that provides high flexibility and scripting features that system administrators use to monitor and send alerts when services in production servers fail. We saw the wide use of Nagios in pagers used in private companies, universities, and medical facilities.

```
ADDRESS]com)  
From: nagios@[EMAIL ADDRESS] Subject: PROBLEM: [EMAIL ADDRESS]/HTTPS is
```

```
CRITICAL - Service: HTTPS Host: [HOSTNAME] Address: xx.xx.xxx.187 State:  
CRITICAL Info: Connection refused Date: Sat+May+7+00:19:35+EDT+2016  
From: nagios@[EMAIL ADDRESS] Subject: (Critical) -[ORGANIZATION].net -
```

```
SolarWinds-[ORGANIZATION].net - ip 172.28.xxx.xx; Volume [DMZ]-/opt at 91 %  
utilization - Node is Critical  
From: nagios@[EMAIL ADDRESS] Subject: PROBLEM: MEDITECH Task Service is
```

```
CRITICAL on host [HOST] PROBLEM: MEDITECH Task Service is CRITICAL on host  
EAT-TS01Servi
```

IntruShield®

McAfee® IntruShield is a next-generation intrusion prevention system (IPS). It scans for known vulnerabilities in networking packets. Intrushield reports the incident through its paging system. By looking at the received pages, we were able to observe and analyze the incident report. Through the incident reports we were able to identify the type of attacks that were being used against a particular company, as well as the source and destination IPs associated with such events.

One of our primary observations was that there were quite a lot of complaints about high IP fragmentation. For us, that seemed to imply that the organization might have experienced a denial-of-service attack or their routers were simply dropping packets. The messages looked like this:

```
From: IntruShield@[EMAIL ADDRESS].org Subject: Interesting Event - IntruShield  
Inbound IP Fragment Volume Too High M3050DMZ SRC: . N/A DST: . N/A n/a 2016-  
01-25 20:46:44 EST
```

We also saw messages about detected attacks, sometimes with respective CVE numbers. It is interesting that the CVE list is quite short, which could possibly mean that the hackers avoided attacking such a high value target with outdated vulnerabilities.

```
From: [NAME]@[EMAIL ADDRESS].org Subject: IP Block - SRC: 134.167.160.67 DST:  
31.13.74.1 directive_event: DIR-Cisco Exploit 10.254.1.248 Alert detail: *
```

- CVE-2016-0068 Microsoft® Internet Explorer® Elevation of Privilege Vulnerability
- CVE-2016-0936 Adobe® Acrobat® Memory Corruption Vulnerability
- CVE-2016-0938 Adobe Reader® and Acrobat Memory Corruption Vulnerability
- CVE-2014-1791 Microsoft Internet Explorer Memory Corruption Vulnerability
- CVE-2016-0007 Microsoft Windows Mount Point Privilege Escalation Vulnerability
- CVE-2014-6366 Internet Explorer Memory Corruption Vulnerability
- CVE-2014-0526 Adobe PDF Reader Encoding DCT Vulnerability
- CVE-2015-1666 Internet Explorer CMetaElement code execution

- CVE-2016-0966 Adobe Flash® Player Memory Corruption Vulnerability
- CVE-2016-0091 Windows OLE Memory Remote Code Execution Vulnerability
- CVE-2016-0098 Apache Server Multiple Vulnerabilities
- Apache mod_cgi Bash Environment Variable Code Injection
- Mozilla Firefox nsFrameManager Remote Code Execution Vulnerability

In addition, our observation allowed us to identify a limited number of LAN IP addresses that were exposed—with four class C networks with 192.168.x.x and one 10.254.14.x. By taking a closer look at the source and destination IP, we were able to gather a few clues on the kind of attacks that were initiated and from what specific IP. With the limited amount of information we have, we were able to make a slight interpretation of how some attacks took place. These interpretations, however, are not definite.

| IP | Domain | Possible Event |
|---------------|----------------------------|--|
| xxx.xxx.xx.54 | [UNIVERSITY].edu | Microsoft Word® wwlib.dll Heap Buffer Overflow |
| xxx.xx.xxx.73 | passivefranchiseincome.com | Maybe someone browsed an advertisement |
| xx.xxx.xx.28 | [ORGANIZATION].gov | Browsing a PDF on the site |

Table 1. IP address, domain and possible event by correlation

WINS, Oracle, Password and Exposed SQL Query

In some paging messages we found WINS names, server names of Microsoft SQL Server and Oracle Database, as well as passwords and error messages with SQL query. The exposed WINS names is equivalent to LAN IP and hostnames. The messages looked like this:

```
Fr:sql_dba@[ EMAIL ADDRESS].Su:SQLdm Alert (Critical) - Clustered server [HOSTNAME]
\] ContentDB1 failed over from ecmsqlxtn1 to ecmsq. 4/29/2016 1:48:14 PM, Cluster
Failover on ECMSQLEXT1\ContentDB1 is Critical.
```

```
INITIAL T3242488 UEM 8882000549X1 FLDP1LREIQD19 - MSSQL_SERVER_DB [NETBIOSNAME]\  
[SERVER].COFEEFRAMEWORKLOGGING LOGSPACEUSEDPCT GREATER THAN Sent At 00:24
```

```
From: nagios@[EMAIL ADDRESS].org Subject: PROBLEM: Enterprise SQL Cluster instance/  
SQL Server is CRITICAL - Service: SQL Server Host: tigris-sps Address: xxx.xxx.  
xxx.234 State: CRITICAL Info: MSSQLSPS: Stopped Date: 03-05-2016 10:41:07
```

```
Sub: Failure: [NETBIOSNAME]\MSSQLSERVER2008 Critical Alert Backup failed Frm: zzD-  
BAs@[COMPANY].com
```

```
From: [NAME]@[ORGANIZATION] Subject: 47814: - [NETBIOSNAME] service 'SQL Server  
(MSSQLSERVER)' is Down Responses: Acknowledged, will work on it Not able to respond  
Resolved
```

```
CONFIRM | | eReID: E080, | | De/From: "MSSQL S00DBP102" <[NAME]@[COMPANY].com>, |  
| Sujet: SQL Server Job System: 'Backup all databases logs Set 02' completed | O/C :  
[NAME]
```

In rare cases, we saw passwords transmitted through pagers. These are easily available and practical information that a hacker can exploit. Such a page would look like the following:

```
n%t change the password! Try #1234abcde#. He zapped it. It should work now
```

Getting a hold of information such as SQL queries, paths, and the brand of database in error messages are useful to hackers since those types of information make it easier for them to exploit vulnerabilities and perform SQL injections.

Personal Paging Messages

Personal messages sent via paging gateways are in fact very valuable since such messages can help an intruder figure out the kind of relationship different parties have. The leaked pages can also reveal personal events involving the concerned parties, which hackers can use to craft fraudulent messages.

```
From: CC_Message_Notification@usamobility .net - [EMAIL ADDRESS]:You guys go ahead. I'm eating here. [NAME]
```

```
From: CC_Message_Notification@usamobility .net - [EMAIL ADDRESS]:Hi [NAME], [NAME] from photography here. I'm leaving in just a minute to meet you at [PLACE]. If you need to call real quick, [CELL PHONE NUMBER]
```

```
From: CC_Message_Notification@usamobility .net - [EMAIL ADDRESS]: [NAME] taking your father to emergency room Ft [PLACE] near [PLACE], car accident, he is hurt but talking [NAME]cell [CELL PHONE NUMBER]
```

Possible Attack Scenarios and How Leaked Pages can be Misused

Through the leaked information found in pages, the main attack scenario we have in mind is highly related to social engineering. This scenario is likely to happen as social engineering is frequently used for reconnaissance and is also used as the main stepping stone for an attacker to gain a foothold in the targeted organization's network. To support the idea of social engineering being used as an attack scenario, we will provide examples of leaked paging messages that are modeled after the pages we observed during our research.

Many facilities using the aforementioned systems—such as hospitals, critical infrastructures, related companies and organizations, and even industrial environments—can be considered high profile targets because of the sensitive nature of the information they hold and because of the processes they control. In this section, we will list possible attack scenarios that attackers can use. Even so, attackers may still come up with attacks that are much more creative and destructive.

For us, we believe that the following can be some of the main goals of every attack:

A. Reconnaissance

1. Collect passive intelligence of hostnames and intra-network topology.
2. Join an internal conference with authentic conference code.
3. Collect intelligence on the target's friends, appointments, days off, etc.
4. Collect intelligence on the target's organizations in terms of interpersonal relationships and club activities.

B. Use gathered intelligence toward other ends

1. One option is to fake personal events. For example, attackers may send a message like “your father was in a car accident” as we have described earlier.
2. Fake intimate messages that could cause personal troubles to targeted officers.
3. On a more serious scale one could imagine an attacker using this type of information to actually cause damage within the facility or as a first step toward a targeted attack. Given the abundant paging messages in clear text and the amount of detail they provide content-wise, the options are wide.

Social Engineering

Kevin Mitnick, author of “The Art of Deception” and “The Art of Intrusion”, discussed different ways for a skilled hacker to conduct social engineering. Given the types of paging messages we reviewed, we were able to understand how hackers can penetrate a facility by using information gathered from leaked pages. One of the ways an attacker can use information found in pages is to, for example, impersonate a contractor who needs help fixing a faulty access badge.

```
[NAME] [OFFICE NAME] locked down as soon as I got to the gate. I am back in my  
office. Didn't come through 8 for fear of my badge not working. You can put me on  
speaker/conference call if you need me. Sorry. [NUMBER]
```

If the scenario of a malfunctioning badge is not effective, then perhaps a message talking about the sale of flea meds or an invitation to a Bible study will work.

```
FROM: [EMAIL ADDRESS] SUBJECT: REMINDER: Invitation: flea meds for dogs @ Monthly  
on day 2 [EMAIL ADDRESS] BODY: 12:00:00 AM-12:00:00 AM
```

```
FROM: [EMAIL ADDRESS] SUBJECT: BODY: (2/2) 12:00-13:00 “Bible Study” @729/Chil-  
laboration ... 13:30-18:30 “Reserved”
```

The messages above are calendar reminders. This would give an attacker interesting clues about what their target is interested in and what he is doing or where he will be on any given day.

Passive Intelligence

In the paper we released discussing the risks related to pagers in industrial environments, we talked about passive intelligence being used there.⁴ Passive intelligence is information gathering as opposed to active intelligence, which requires an attacker to make some kind of contact with the target's network. For attackers, using passive intelligence to penetrate a facility or an organization is better since it is not as risky as using ping and port scanning to find open ports on servers or perhaps calling someone in the facility to social-engineer classified information—as both ways can alert people in the facility. With passive intelligence, attackers will only have to wait for available information from intercepted pages, analyze the information, and then perform a penetration test or carry out an attack.

As it turns out, pages are considered a source of high quality passive intelligence. During four months of observation, we saw messages containing information on contact persons, email addresses and phone numbers, locations inside manufacturers and electricity plants, thresholds set in industrial control systems, intranet IP address, intranet hostnames, and much more. Looking at the different gateway software programs, we came across several gateway programs that could easily allow an attacker to collect enough information to create a phonebook of significant people working in a facility. In this section, we will describe how an attacker may build a phonebook specific to an organization and then construct messages to social-engineer information from important people listed in the phonebook.

Recon on employees working for government critical services

Let us take the example of a simple email-to-pager gateway message. In the “FROM” field of an email-to-pager gateway a person's email address and the facility he/she works for can be seen. Here we saw a message from a user we'll identify as Annie, who is seen sending a message about a business trip. This particular assumption was made based on the paging message about the Marriott Hotel. This is what the message looked like:

```
FROM: [Annie]@[ORGANIZATION].org SUBJECT: BODY: JW Marriott is $319 a night.  
The allowable is $226. Do you want to pay the difference? [Annie]
```

Although Annie's last name was not shown, most attackers could easily find additional information about a particular individual by either intercepting more paging messages or by checking out social media profiles of people with similar names—such as a LinkedIn profile. For most attackers, identifying an individual with only a few details is easy. With information, such as an individual's name, age, job title or function, company or organization name, addresses, and telephone numbers, available on most people's social media profiles hackers can effectively craft social engineering strategies to hack an individual. If we take the data described below, for example, here are a number of scenarios that we think are possible:

- **Name, Email, Contact Number:** We saw people’s names, emails, and contact numbers in pages. By getting a hold of the contact numbers, hackers can easily pretend to be part of a facility or an organization. For instance, hackers can impersonate an employee once they get a hold of sensitive information.

```
NUMBER] * Type:SNT SR Owner: @ ILS Subscription Information: * Subscriber:  
[NAME]@cisco.com
```

- **Most frequent senders:** By looking at the email addresses from received or sent paging messages, it is easy to determine the individuals who are frequently sending messages through pagers. Attackers can abuse this kind of knowledge by operating under the certainty that these frequent users will always assume that the pages they are receiving are genuine and trustworthy. Through this, frequent users are prone to fall victim to fraudulent messages.

In order to study whether there is a fixed relationship between callers and callees in a WhosCall system, we looked at 108 cap codes that belonged to 68 people in an organization. It is important to note that there may be times that a person may have more than one cap code. During our observation we saw 436 callers who called and we found out that there are some callers who maintain constant communication with a certain individual, thus making them assume that the message is from their contact and that it is credible. For example, a person who constantly exchanges messages with his wife (who also has her own cap code), will always assume that it is his wife contacting him when that particular cap code is used.

Aside from noticing a fixed pattern of communication between two people, we also discovered that there are people who have a wide network of contacts while there are also some people who don’t—as these people tend to call around one or two people only on a regular basis. We believe that people with a broad network of contacts, or high centrality, are likely to become targets of attackers who aim to build a phonebook for social engineering purposes.

CallerID and creating a phonebook

During the course of our study, we found paging messages sent for every missed call. Inside the page, information such as the callee’s email, the cap code, and the caller’s name (or number, if the name is not in the phonebook) are included. By correlating these records with data gathered from WhosCalling, recovering the caller’s phone number is quite easy.

```
From: [NAME]@[ORGANIZATION].org Subject: Missed Call - Missed call from  
[NAME]
```

```
From: [NAME]@[ORGANIZATION].net Subject: WhosCalling - 03/29 09:08 [PHONE  
NUMBER] [NAME]
```

For any attacker, creating a list of people working in a certain facility is beneficial as it will help advance an attacker's plans to draw important information from these contacts through social engineering. With a phonebook, an attacker could easily fake an email, a phone call, or even a page message. An attacker can send a page, for example, that could urge an individual to come home and leave the building just so the attacker can continue with his/her business of getting information. With such tactic, an attacker may use that opportunity to trigger an attack. Below are a few steps describing how an attacker can benefit from creating a phonebook with valuable contacts:

1. The first thing an attacker could do is compose a comprehensive phonebook of the targeted organization. An attacker could use information gathered from entries found in the WhosCalling records or perhaps from the pages that leaked information such as employee names, contact numbers, addresses, etc. The phonebook would not only contain office numbers, but sometimes home numbers and cellphone numbers as well. Sometimes even the number of an operator/control room in an organization can be found in the pages, which enables a skilled social engineer to make a call and collect more valuable information.
2. The second step would be to correlate the phonebook with the "Missed Call" records. With such information we can come up with a pattern off who is calling who and the frequency of calls. During the research period, we observed a total of 2,173 missed calls. We also found that having a voice recognition system can also give an attacker more clues to the identity of the caller and/or the callee.

Voicemail Content Transcription

Voicemail summary systems compile incoming voicemail messages and some can also give the callee the transcript of the first few seconds of a voicemail—making it easier for the receiver to know whether the call is important or not. The system is very helpful, yet it should be considered highly insecure, as it transcribes the content of one's private call. Several voicemail services, such as Google Voice™, provide such function by making your voicemail searchable. Therefore, we would not recommend using such service in any environment where security and confidentiality surpass usability. Fortunately we haven't seen the use of such voicemail systems in either the healthcare sector or industrial control systems.

This is a voicemail summary similar to the one we saw:

```
FROM: [NAME]@[ORGANIZATION].orgSUBJECT: BODY: Voice mail:11s from [PHONE NUMBER].  
Hey . Hi she just just missed your call. You want tell me what's up give me a call  
back bye.
```

The callee's email, length of the voicemail, CallerID, and a short transcript are provided in this page. In other systems, the format varies a bit, but the core idea remains. As it is considered polite in most social settings to address the callee and the caller by name, it is easy to see who is calling who.

```
FROM: [NAME]@[ORGANIZATION].org SUBJECT: BODY: Voice mail:34s from [NAME] @  
[PHONE NUMBER]. Hi David hi this John H. it's Friday afternoon at 2:00 I just  
wanted to ...
```

Parcel Tracking

In the previous paper in the series, we showed how some pages contained FedEx® tracking numbers. In the first two papers of the series, we emphasized the risk of collected or stored information being leaked.

| Tracking No. | Shipper city, state | Origin Terminal | Ship date | Recipient city, state | Delivery date |
|--------------|---------------------|-----------------|-----------|----------------------------|--------------------|
| XXYXYX4318 | Whiteman AFB, MO | SEDALIA, MO | 2/29/2016 | PALMDALE, CA | 3/01/2016 9:57 am |
| YXXYXY8272 | Whiteman AFB, MO | SEDALIA, MO | 3/04/2016 | REDONDO BEACH, CA | 3/07/2016 11:01 am |
| YXYXYX6598 | Whiteman AFB, MO | SEDALIA, MO | 3/08/2016 | HONOLULU, HI | 3/09/2016 12:36 pm |
| XXYXYX5811 | Whiteman AFB, MO | SEDALIA, MO | 3/10/2016 | PALMDALE, CA | 3/11/2016 10:34 am |
| YXYXYX1721 | WHITEMAN A F B, MO | SEDALIA, MO | 3/10/2016 | ALBUQUERQUE, NM | 3/11/2016 9:57 am |
| XYXYXY7126 | Whiteman AFB, MO | SEDALIA, MO | 3/14/2016 | EL SEGUNDO, CA | 3/15/2016 10:23 am |
| XXYXYX8229 | Whiteman AFB, MO | SEDALIA, MO | 3/25/2016 | TINKER 1 F B, OK | 3/28/2016 10:04 am |
| YXYXYX4552 | WHITEMAN A F B, MO | SEDALIA, MO | 4/05/2016 | HIAWATHA, IA | 4/06/2016 9:16 am |
| YXYXYX9162 | Whiteman AFB, MO | SEDALIA, MO | 4/07/2016 | EL SEGUNDO, CA | 4/11/2016 7:50 am |
| XXYXYX4580 | Whiteman AFB, MO | SEDALIA, MO | 4/12/2016 | PALMDALE, CA | 4/13/2016 9:46 am |
| XYXYXY4754 | Whiteman AFB, MO | SEDALIA, MO | 4/21/2016 | YUKON, OK | 4/22/2016 12:42 pm |
| YXXXXY4032 | WHITEMAN A F B, MO | SEDALIA, MO | 4/28/2016 | ALPHARETTA, GA | 4/29/2016 12:00 pm |
| XXYXYX9862 | WHITEMAN A F B, MO | SEDALIA, MO | 5/02/2016 | HIAWATHA, IA | 5/03/2016 9:19 am |
| XXXXXY2456 | Whiteman AFB, MO | SEDALIA, MO | 5/03/2016 | WRIGHT PATTERSON A F B, OH | 5/04/2016 10:36 am |
| YXYXYX5597 | Whiteman AFB, MO | SEDALIA, MO | 5/04/2016 | EL SEGUNDO, CA | 5/05/2016 10:11 am |
| YXXXYX8026 | WHITEMAN A F B, MO | SEDALIA, MO | 5/05/2016 | SMITHTOWN, NY | 5/06/2016 10:06 am |
| XYXXXX9029 | WHITEMAN A F B, MO | SEDALIA, MO | 5/05/2016 | SMITHTOWN, NY | 5/06/2016 10:06 am |
| XYXYXY3646 | WHITEMAN A F B, MO | SEDALIA, MO | 5/05/2016 | EAST GREENWICH, RI | 5/08/2016 9:42 am |
| XYXYXY2349 | Whiteman AFB, MO | SEDALIA, MO | 5/05/2016 | IRVING, TX | 5/08/2016 10:22 am |
| XXXXYX3409 | Whiteman AFB, MO | SEDALIA, MO | 5/05/2016 | LINCOLN, NE | 5/08/2016 11:30 am |
| YXYXYX9514 | Whiteman AFB, MO | SEDALIA, MO | 5/11/2016 | GREENLAWN, NY | 5/12/2016 10:30 am |

Table 2. A sample list of FedEx shipment details modeled after what we saw in the pages

In the table above, we recreated a facility's pattern of shipment for three months—which is similar to what we saw in the pages we observed. Tracking numbers as well as specifics like places and delivery dates were, of course, just part of the bits of information that were available. While we, or any outsider in particular, may not have a clue of what these parcels contain, an insider—or a person who is familiar with what's going on in the industry the targeted facility is a part of—may have an idea of what the parcel may contain. This type of information can be used to claim insider status, manipulate the delivery of the package or information on the recipient etc.

Passcodes Transmitted in Clear Text

Another rather astonishing type of leaked information are passcodes transmitted in clear text. We found these types of leaks in pages among health care organizations, banks, and energy providers. To our surprise, we also saw Microsoft Outlook® Web App (OWA) passcodes sent as pages too.

Conference Bridges

The most common passcodes in our observation are conference bridges. Imagine a hacker or an industrial spy dialing in and silently listening to every single detail in a conference call. The host does not always bother to check whether everyone in the call is authorized; thus a hacker has a good chance to remain unnoticed. We saw examples of the transmission of such information with a major energy provider, a bank, and a major provider of advanced digital satellite telecommunications and wireless signal processing equipment.

```
Within EPIC, you are listed as the ordering/attending provider;therefore an amcom  
was sent. Call [PHONE NUMBER] passcode xx4994 for a YELLOW CRITICAL RESULT. Sent  
via amcom on 5/18/2016 @ 6:16 AM. [27]
```

This is an example of a page containing a passcode that concerns a major energy company that also owns several nuclear plants:

```
From [NAME]@[ORGANIZATION].com Sub:2205 SLT Call for [NAME] with cooling water  
isolated [PHONE NUMBER] Passcode xxx495
```


Microsoft Outlook Web App

Microsoft OWA passcode⁵ works just like the two-factor authentication process—except it does not change every minute. It is designed to make the access to mailboxes more secure. In addition to a username and a password, one has to type their OWA passcode, if activated, thus making the mailbox more secure against credential phishing.

However, OWA passcodes sent paging messages weaken the protection. For a hacker, access to passcodes just opens up a list of candidates to phish.

```
FROM: [NAME]@[FACILITY].org SUBJECT: BODY: Your passcode is xx0923. Enter this  
number in Outlook Web App to set up notifications.
```

```
FROM: [NAME]@[FACILITY].org SUBJECT: BODY: Your passcode is xx4087. Enter this  
number in Outlook Web App to set up notifications.
```

Conclusion

Our research throughout different areas—from the healthcare sector, to ICS environments, and now a broad array of organizations that utilize certain IT systems—confirms an overall theme: there is an enormous amount of information that is being transmitted through pagers in clear text, without any type of encryption. Given the privacy violations this type of leakage would constitute and the security concerns it raises, we are surprised to see how organizations and enterprises have overlooked the security of their pagers.

If pagers cannot be substituted with more secure technologies, information sent through these pages, which can give distinguishing clues about an organization, must be properly encrypted or protected. The first step toward achieving that is employing adequate encryption.

Here are few baseline recommendations we offer to various organizations and/or enterprises that are still using pagers to communicate sensitive information:

1. First and foremost, we recommend organizations and/or enterprise to switch to a more modern means of communication that has better security standards in place instead of using a legacy system that is plagued with severe problems like leaking information.
2. If it is absolutely unavoidable to use pagers to communicate, organizations and/or enterprises must make sure that any information sent through such devices is encrypted.
3. Any encryption or security method applied to pager communication needs to uphold the overall security standards of a facility. While there are external regulations each organization or facility are compelled to follow, every facility or organization may opt to apply certain regulations on a case-to-case basis.
4. Do not address your callee's name even though it may seem impolite. Malicious actors can extract your contacts using the information

5. Avoid transmitting passwords through a technology that's not secured, such as pagers.
6. Avoid using voicemail transcription services and automated summary systems if you can.
7. Conduct a thorough assessment of the risks involving the use of pagers, and other legacy systems, in communicating sensitive information. For facilities dealing with sensitive information, a thorough and comprehensive risk assessment is paramount. People in charge of conducting security assessments must weigh the risk against the benefit of using pagers to send information. In addition to being a major violation of privacy laws, pager systems spilling sensitive information also brings forth major security implications.

References

1. Process Flows. (n.d). *ProcessFlows*. "CX-E Unified Messaging." Last accessed on 11 September 2016, <https://processflows.co.uk/unified-comms-sms/products/cx-e/mobile-applications/cx-e-unified-messaging/>
2. 9-1-1 Magazine (14 July 2014) *9-1-1 Magazine*. "USA Mobility Announces Name Change to Spok." Last accessed on 11 September 2016, <http://www.9-1-1magazine.com/Corp-USA-Mobility-Changed-to-Spok?TopicID=522>.
3. Ipswitch. (n.d.) *ipswitch*. "WhatsUp® Gold 2017 is IT monitoring reimagined." Last accessed on 11 September 2016, <https://www.ipswitch.com/application-and-network-monitoring/whatsup-gold>.
4. Stephen Hilt and Philippe Lin. (25 October 2016). *Trend Micro*. "Leaking Beeps: Unencrypted Pager Messages in Industrial Environments?" Last accessed on 11 September 2016, https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_leaking-beeps-industrial.pdf
5. Microsoft Office Support. (n.d.) Microsoft. "Outlook Web App options on a mobile device." Last accessed 11 September 2016, <https://support.office.com/en-us/article/Outlook-Web-App-options-on-a-mobile-device-eea5e255-54ef-4319-ad9b-98764c925a03>.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud

www.trendmicro.com