As work-at-home increases, so do attacks on VoIP and unified communications

BY ZEUS KERRAVALA, NETWORK WORLD

Businesses use on-prem and cloud-based unified communications (UC) to connect distributed workforces but often don’t realize the security threats hidden within popular UC services, but they should, and they should address them.

There has been a sharp rise in eMeetings, Voice over IP (VoIP) and other UC capabilities as companies shift to a work-from-home (WFH) model because of the COVID-19 pandemic. Don’t expect this trend to abate anytime soon as 93% of CXOs that responded to a ZK Research study say they see a permanent 30% uplift in the number of remote employees.

Survey respondents say maintaining productivity is the top challenge when shifting users to WFH, highlighting the importance of collaboration tools. The right ones can make the transition seamless. For example, VoIP enables workers to maintain the same phone number at home as they do in the office. They can also connect using a desk phone, mobile phone or software client on a computer, which makes the shift nearly frictionless.

VoIP and SIP attacks on carrier and enterprise networks are increasing rapidly. Robocalls from botnets originate from legitimate servers or rented servers to launch dangerous attacks globally over SIP infrastructure.

On any given day, carriers and their enterprise customers face more than 40,000 different VoIP/SIP attacks, according to research from the RedShift Networks. In addition to robocalls, networks are vulnerable to cyberprobes, registration hijacking, and distributed denial of service (DDoS) attacks.

From my conversations with network and security professionals, the 40,000 number seems on the conservative side, particularly now with the exponential rise in home workers. The growth in the number of people using VoIP services has created a massive opportunity for threat actors and a spike in malicious activity focused on UC systems. This has been a problem long ignored by businesses and service providers but needs to be taken seriously.

New standards have emerged to combat UC threats

The Federal Communications Commission (FCC) and international regulators are tackling the problem by mandating that carriers adopt SHAKEN (Secure Handling of Asserted information using toKENs) and STIR (Secure Telephony Identity Revisited) standards. SHAKEN/STIR targets automated messages delivered via hijacked VoIP and UC-based computer systems. So, calls traveling through interconnected phone networks have their caller ID verified as legitimate before reaching end users.
But not all bogus SIP calls are easily detected. SIP carries all forms of media, not just voice. Various apps like chat and videoconferencing use SIP. Therefore, simply whitelisting or blacklisting IP-based communications is not enough. Businesses must focus on protecting their VoIP systems much like they do their data networks to tackle this growing cybersecurity challenge.

**Protecting communications requires a multi-pronged security approach**

A combination of SIP security, threat intelligence, actionable analytics, and automated fraud detection can improve visibility into unauthorized activities throughout VoIP networks and UC apps. SIP security is necessary to identify and prevent threats at the edge – or entry point – of the network, while threat-intelligence and analytics allows for fast troubleshooting and threat mitigation. Fraud detection and ultimately remediation are needed for real-time monitoring of threats discovered inside the network.

Some UC threat-management solutions are designed specifically for VoIP cybersecurity and implement SHAKEN/STIR standards. They work with protocols such as SIP, real-time transport protocol (RTP), transport layer security (TLS), and secure real-time transport protocol (SRTP) to validate callers beforehand and ensure their legitimacy. Carriers with enterprise customers have turned to such solutions to tackle key problem areas like theft of UC services, costly DDoS or TDoS attacks, robocalls, and VoIP troubleshooting.

Heavily regulated industries are also using UC threat management to maintain compliance by establishing a baseline for normal activity at the SIP/VoIP protocol level. With UC threat management, unique algorithms are used to verify authentic users and block anomalous VoIP/SIP communications or attempts from unregistered users. Healthcare and financial services are two examples of industries where compliance-level protections are required for all communications.

Earlier this year, the FCC issued an order requiring all providers of originating and terminating voice services including VoIP to implement STIR/SHAKEN in the IP portions of their networks by June 30, 2021. Vendors continue to invest in SIP security, as more businesses move to the cloud and adopt UC.

VoIP/SIP attacks on carrier and enterprise networks aren’t going away. Strengthening VoIP security should be a priority. Without security analytics and real-time threat management for UC, businesses could be putting themselves at risk and not meeting their industry’s compliance requirements.

**Zens Kerravala is the founder and principal analyst with ZK Research, and provides a mix of tactical advice to help his clients in the current business climate.**

---

© Copyright 2020 by Network World, Inc., Southborough, MA 01772-9108 • Reprinted from NetworkWorld.com • Trademark is owned by International Data Group, Inc. #C56887 Reprinted by The YGS Group, 800.290.5460. For more information visit www.theYSGroup.com.