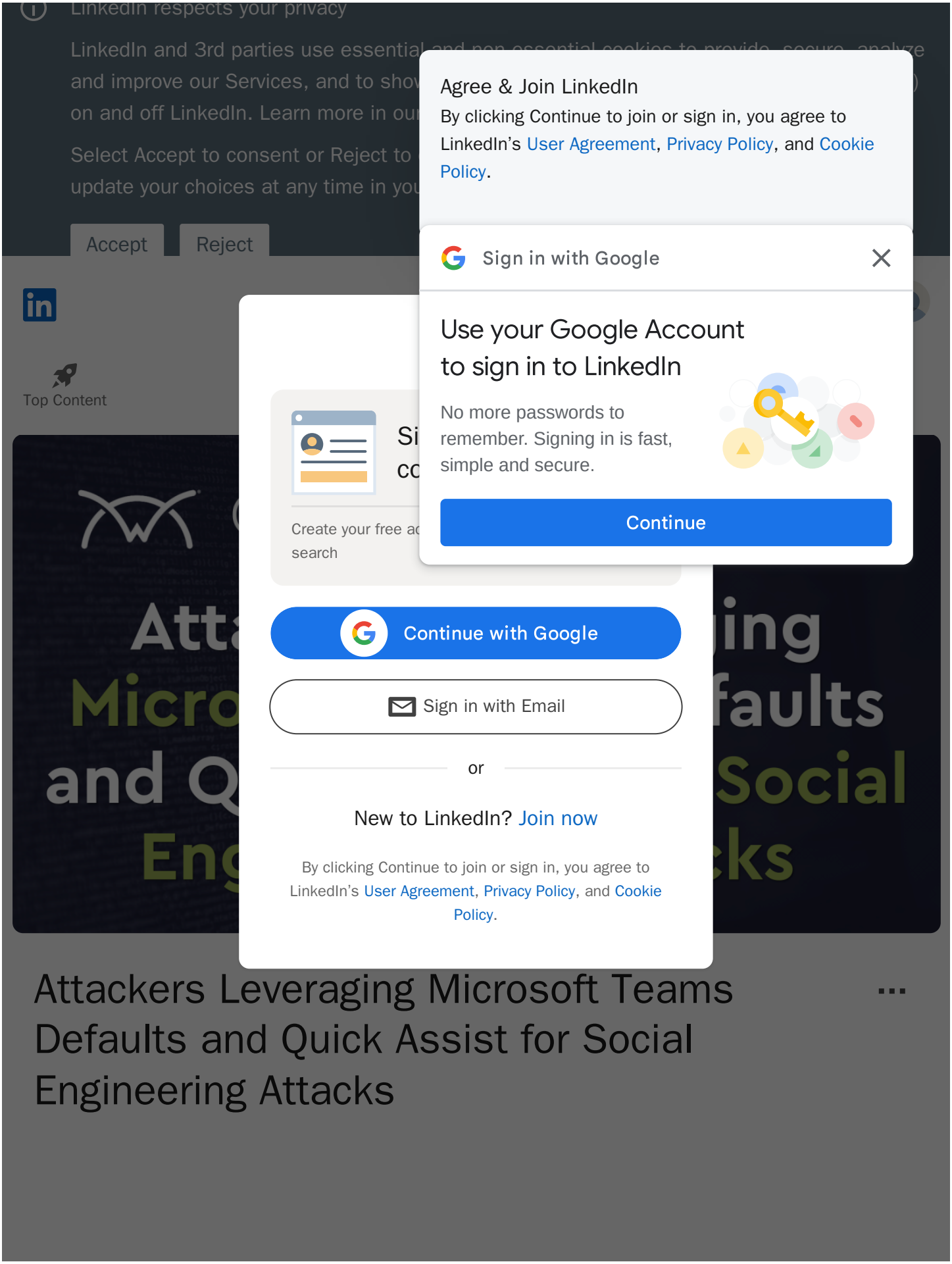


Attackers Leveraging Microsoft Teams Defaults and Quick Assist for Social Engineering Attacks

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show ... on and off LinkedIn. Learn more in our ...

Select Accept to consent or Reject to ... update your choices at any time in you...

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

During January the CRU observed incidents in which phishing was carried out by sending Teams mes... 5 tenant. In this way, they masquera... nternal IT help desk and instructed the v... er to provide the attackers with acces... ccomplished, the attackers used a va... laterally, and elevate privileges.

A similar campaign ... cember of 2024, which they track as ... covered by Microsoft around Ma... m-1811. Both of these reports menti... ware, however, the follow-on activity lea... between what was reported by Microso... phos since November.

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

We are ... ring and mitiga... itional obs... ed.

Initial Access

The attackers sent messages to victims via Teams with a display name of Help Desk. Teams logs all showed the messages coming from different accounts across incidents, but consistently from the same IP addresses of either 78.46.67[.]201, as also reported by Sophos, or 2a01:4f8:120:53f6[::]2, which appears to just be the IPv6 address of the same host. Other reporting outlines a technique of flooding

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (if you accept) on and off LinkedIn. Learn more in our Cookie Policy.

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

archive file pack.zip.

Persistence and Comm

Attackers set the re list of Command and Control (C2) ad rmatted normally, and in others the '.' aced with 'A'. Then they looked specific list.

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

They extracted pack llowed by using the expand utility to extr \OneDrive. This is the native folder for e attackers extracted several ac there, where they would not normally b OneDriveStandalone n to initiate dll sideloading of malic

This behavior was w payloads were also explored by researcl uggested possible ties to Qakbot, whic 31. In both reports exploring the malici oned them coming from a sideload of winhttp.dll. We did not directly observe this, but did see the use of a wscapi.dll file that suspiciously had an original file name of ieui.dll, but had a code signing certificate with a subject name of Farfield Computing Systems Inc. The malicious payload set persistence in the Startup directory with OneDriveUpdate.lnk.

On the beachhead hosts that the attackers gained initial access on we observed these actions being manually executed via a cmd session. They would repeat these steps on several other machines in the environment to establish further footholds

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (if you accept) on and off LinkedIn. Learn more in our Cookie Policy.

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

possible persistence.

On some hosts the URL for downloading the Ate of cynthia.guerrero@st n super market. This suggests they r astructure to further develop their own.

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

Lateral Movement and

The attackers used including RDP, SMB, WMI, WinRS, re observed tampering with the H minal Server\fDenyTSCon HKLM\System\Curr Admin registry keys in order to ease rem).

We were able to ide l movement, such as winrm-fs a tool fo served the use of impersonate, a toke tokens, but also to execute commands controllers, like using the net comm rgeted DCs.

The attackers did use Psexec during an incident, but it was only used to execute commands locally rather than remotely. A discovery tool called eviltree was also observed that can be used for searching across nested directory structures for keywords or regex.

Defense Evasion

On several machines, before installing their backdoor, we observed the attackers make use of a tool to disable SentinelOne on victim endpoints. We identified the

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show ... on and off LinkedIn. Learn more in our ...

Select Accept to consent or Reject to ... update your choices at any time in you...

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

setting the system date to 2012 before executing k2bi .exe.

It does this becaus... ...ired. Setting the system time somew... ...the Windows Time Service effectively a... ...e certificate.

The controller binar... ...gh a handle it opens to the hardco... the DeviceIOControl API. It initiates com... ...e 0x2236544 and passes it the id "7N... ...Gh20pWUuN1-ZxfXdiOYps6HTp0X"

During execution, k2... ...n the C:\Program Files\SentinelOne d... ...a .exe extension using IOCTL value 0... ...he running processes and kills ... ...36740 along with the corresponding p... ...will idle, looking for a directory named '... ...this directory (or just any file named ... ...running. Otherwise it runs indefinitely.

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

ATT&CK Techniques

Initial Access

T1566.003 Spearphishing via Service

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show [illegible] on and off LinkedIn. Learn more in our [illegible]

Select Accept to consent or Reject to [illegible] update your choices at any time in your [illegible]

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

T1569.002 Service [illegible]

T1047 Windows Ma[illegible]

Persistence

T1098 Account Mar[illegible]

Recommende[illegible]

Email Bombing a[illegible]

Audrey Moreau · 1 ye[illegible]

Sophos MDR Unc[illegible]

Prasad Wijesuriya · 1[illegible]

Upcoming Microsoft Teams "Chat with Anyone" feature…

CyberProof · 4 months ago

T1547.001 Registry Run Keys / Startup Folder

T1136.002 Domain Account

T1574.001 DLL Search Order Hijacking

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show [illegible] on and off LinkedIn. Learn more in our [illegible]

Select Accept to consent or Reject to [illegible] update your choices at any time in your [illegible]

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

T1112 Modify Regis

Discovery

T1087.002 Domain

T1069.002 Domain

T1033 System Own

Lateral Movement

T1570 Lateral Tool

T1021.001 Remote

T1021.002 SMB/W

T1021.006 Window

Command and Cont

T1219 Remote Acce

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

IOCs

IPs

Command and Control:

185.190.251[.]16

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show on and off LinkedIn. Learn more in our

Select Accept to consent or Reject to update your choices at any time in you

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

Teams Phishing:

2a01:4f8:120:53f6

78.46.67[.]201

Teams Phishing Acc

admin_911@stmgny

DDDr@freeagentnet

admin_0123@remic

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

ConnectWise C

57,332 follow

+ Subscribe

Like

42

To view or add a comment, sign in

More articles by ConnectWise

Nov 12, 2025

Patch Tuesday | November 2025

By: Bryson Medlock It's Patch Tuesday! Every 2nd Tuesday of the month, Microsoft and other vendors release regularly…

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show you relevant ads (if you accept) on and off LinkedIn. Learn more in our Cookie Policy.

Select Accept to consent or Reject to decline non-essential cookies for this use. You can update your choices at any time in your settings.

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

AI-Generated Code: The Hidden Security Debt of Automated Development

AI coding tools are accelerating software delivery across every industry, yet nearly

Oct 24,

Critica

By: Br

Servic

dows Server Update

21

Sign in to view more content

Create your free account or sign in to continue your search

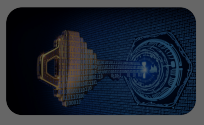
or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

Show more

Others also viev



Mitigatir

Godwill O

The Wea formation Security Chain m

Sandeep

SMBs' Personal Guide to Insider Threats and Social Engineering Attacks

Johnathan Lightfoot · 3y

RomCom Hackers Exploits Windows & Firefox Zero-Day in Advanced Cyberattacks

Ifeanyichukwu Nwonu, MSc · 1y

Everything you need to know behind the TikTok ban and what it means for cybersecurity... Read Luigi's thoughts and more stories below.

Luigi Tiano · 1y

LinkedIn respects your privacy

LinkedIn and 3rd parties use essential and non-essential cookies to provide, secure, analyze and improve our Services, and to show on and off LinkedIn. Learn more in our

Select Accept to consent or Reject to update your choices at any time in you

Agree & Join LinkedIn

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

Ransomware Techniques to Watch Out For
10 Posts · 1,129

How Ransomware Attac
9 Posts · 1,655

Secondary attack vecto
3 Posts · 234

Explore content

Career

Productivity

Project Management

Show more

Sign in to view more content

Create your free account or sign in to continue your search

or

New to LinkedIn? Join now

By clicking Continue to join or sign in, you agree to LinkedIn's User Agreement, Privacy Policy, and Cookie Policy.

© 2026

Accessibility

Privacy Policy

Copyright Policy

Guest Controls

Language