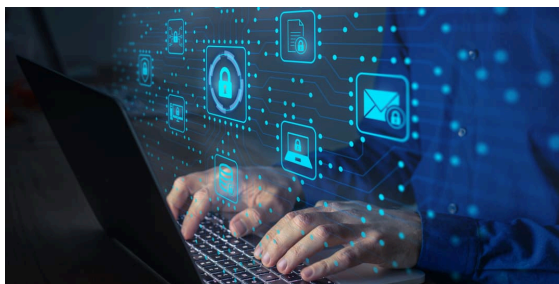


Unwanted Gifts: Major Campaign Lures Targets with Fake Party Invites

security.com/threat-intelligence/rmm-logmein-attacks



- Frequently seen remote management and monitoring (RMM) tools used in these attacks include LogMeIn Resolve, Naverisk and ScreenConnect.
- In many cases, the attackers are using a new tactic that installs additional remote management and monitoring (RMM) tools on infected computers long after the initial compromise occurs.
- While motivation for this tactic remains unclear, it is possible that they are trying to sell access to victims to other threat actors for further compromise, such as ransomware deployment.

A highly active threat actor that specializes in using the ScreenConnect remote management and monitoring (RMM) software in its attacks has changed tactics and is now infecting its victims with multiple RMM tools, including LogMeIn Resolve and Naverisk.

In many cases, the attackers install additional RMM tools on infected computers long after the initial compromise occurs. The motivation behind this new tactic remains unclear, although it appears that the attackers are attempting to increase their dwell time on networks in order to maximise their return on successful attacks.

Its attacks adhere to a consistent pattern, beginning with phishing emails employing a variety of lure tactics. Recent emails have masqueraded as holiday party invites, such as "Party Invitation" or "December Holiday Party". Other email lures have masqueraded as invoices, tax correspondence, payment overdue notices, Zoom meeting invites, or documents to be signed.

Attack chain

The emails contain malicious URLs linking to setup executables or MSI installers. In some cases the installers are signed. Until recently, these files would attempt to install ScreenConnect on the victim's machine. ScreenConnect would then be used to download an additional attacker toolset. The toolset deployed varied, but frequently seen tools included:

- HideMouse.exe: Utility designed to hide mouse cursor movement which can be leveraged by attackers to hide evidence of remote access.
- WebBrowserPassView: A [password-recovery tool](#) that reveals the passwords stored by multiple web browsers.
- Defender Control: A tool for [disabling Windows Defender](#).

The nature of the toolset suggested the attackers wanted to cover their tracks, disable security and harvest credentials for further exploitation. Other tools deployed that have yet to be analyzed include files named Hidefromcontrolpanel, PhoneLinkLauncher, and Windowsspasskey.

Changing tactics

The campaign has been underway since at least April 2025. Initially the attackers focussed exclusively on distributing ScreenConnect and then using it to deliver the secondary toolset. However, the attackers have since modified their tactics and are now installing a wide range of other RMM tools on compromised machines in addition to ScreenConnect.

Beginning in June, the attacks also began installing SimpleHelp along with ScreenConnect. Beginning in late August, they began deploying PDQ and Atera in addition to ScreenConnect.

Most recently, since October, the attackers mainly seem to be using LogMeIn Resolve (formerly GoTo Resolve) and another RMM package, Naverisk, along with ScreenConnect.

Interestingly, the RMM tools are usually not installed simultaneously. Instead, one is used to install another and often a period of time can elapse between installations.

For example, one organization was initially compromised with ScreenConnect installed in August 2025. The installer had a masqueraded file name: document.clientsetup.msi. The attackers later made use of the installed ScreenConnect to download additional tools onto the machine. On September 20th, another version of ScreenConnect was installed (ConnectWise). On September 21st, LogMeIn Resolve was also installed, using a masqueraded file name. (adobereaderdc.clientsetup.msi)

In another case, an organization was first compromised with LogMeIn Resolve on October 31, 2025. This was immediately used to install ScreenConnect which was then used to deploy additional tools including HideMouse and WebBrowserPassView. On November 6, the Naverisk RMM was also installed on the same machine.

Maintaining access?

The strategy behind this new tactic remains unknown. One possibility is that the attackers believe that they are less likely to be detected if they continually change their toolset and by installing additional RMMs they are creating some level of redundancy. Another possibility is that they may be using trial licences for these RMM tools and regularly need to switch them to avoid them expiring.

The end goal of these attacks are unclear, however, given that the attackers are prioritizing persistent access and credential theft, the most likely explanation is that they are selling access to victims to other threat actors for further compromise, such as ransomware deployment.

Protection/Mitigation

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

4abe29bbcb4458ef5abdecdfcaaf3837d0a15321a49bc97c20310f92f76b84a2 – ScreenConnect MSI

1a534d04bf30894d20764e91f7e94e0a73f060f0abacc9feedba427995c83a8 - HideMouse

6cc665057c4a4fe42a309afd3a7fa96cf1af126e9c6e08e56df5105e05378bcc - Hidefromcontrolpanel

36541fad68e79cdedb965b1afcdc45385646611aa72903ddb9d4d064d7bffb9 - Webbrowserpassview

499d07894f730fb685ee3cbfc1a933e0da93750c1ed25a49b2eb9c32adef156a - PhoneLinkLauncher

18399555137b889a51eb543ddf01b3b7471a6e20453ee24801f8895528e7632f - Windowspasskey

a93c946c237b981189d2668d938a9d4d1d9681757e48dae8d9d65ed25b5da657 - Windowspasskey

bfa9c3298a749c8949f890ef02b4d07589bea1635150d57215b2f37b6f3acef0 - Defendercontrol

951d9bd7842cbd6c31f57e271bccc624f0d8285a713b87ab928145930162f625 - LogMeIn/Goto Resolve MSI

9c6621b2ac227cc08878fa058d803f9fb067462f667400fd1854dc017405c933 - LogMeIn/Goto Resolve MSI

8c725c1f37a37d536673042abe7a06ed87407adb3399d0b570f6690d341ff0ed - LogMeIn/Goto Resolve MSI

98ea70b86512e58b6ecb79d7ad55e808215977d13b5626d9661f962f36861109 - LogMeIn/Goto Resolve MSI

4ca1746d65c9864ec9e55620a41baf55997d40c7cc0b6474be4c222100744063 - LogMeIn/Goto Resolve MSI

111a3dc067f3e47ee9b8188219e410a1f83a54133813ca01592563e575c82dfa - LogMeIn/Goto Resolve MSI

302ebfb06504b2510880bf1019bd9984708a2c019eea3b0b3134d45f874d7178 - LogMeIn/Goto Resolve MSI

e2b2455927f33f7029aa6583ddf397fb2236e0ee7b2088bf5720d28b6b1c4467 - LogMeIn/Goto Resolve MSI

ac3fb3616cf4617d2c1dcfedc6f2950d01f5d4e3b9b351f7cf16758bb1e63e66 - LogMeIn/Goto Resolve MSI

9c626bff599de35fed597f85bd010a7d5dc7e9d1fc2936c76023e78c38f4da3b - LogMeIn/Goto Resolve MSI

32c3b6236990001bfc1c8da1a97f164681134fb59dc28ff21d3744fb85571c81 - LogMeIn/Goto Resolve MSI

b06c79e17994872ec5693269bd78ea740e1604ff8a8f588f0fc88d2b3be3338a - LogMeIn/Goto Resolve MSI

347606a44f63c87f1331d313d65971f8ec97127762b393f420d2965a470f45b3 - LogMeIn/Goto Resolve MSI

70e2806fe1b337048af22567fa4783fb7fddcae981a57c75b30cc9c6b9303ae5 - LogMeIn/Goto Resolve MSI

729f6c1661dfb40a4d71a1e1131dc1b3c707473bab92a24982235f58e56abfd - LogMeIn/Goto Resolve MSI

44246110b60cd7231d3a8bac35e697fe0cf55317923980e7424dc1dd0dbea808 - LogMeIn/Goto Resolve MSI

c743ac8eeb089864bb8638c46adc1e0eee48ea917e2eb8c8192b2783f9db82d4 - LogMeIn/Goto Resolve MSI

b32bc15db7a2f0340a5459b92eab1fe515eb07da97d81a91fd743e5591a333cb - LogMeIn/Goto Resolve MSI
1cc0e73600b6b620c767d490419052bcd2597e153321f7c8f8f5b026d7faaa3 - LogMeIn/Goto Resolve MSI
48470b2eff64cfcb11684152ae6101c930317e0912a10ce052e3b53d0fa48efe - LogMeIn/Goto Resolve MSI
e11d7e4cb3a05de7f9a7ad6a3277fb1133008f322be857a87abe02ec041de963 - LogMeIn/Goto Resolve MSI
bbc7f54e9e66a66b72f9e184c5b317c250e8c23f0aa28aca9e3a61ebb89c9c72 - LogMeIn/Goto Resolve MSI
e1b4a079e65719be651cfc249913ac07ac3e0ae58715e7435eed5a5ef1df6626 - LogMeIn/Goto Resolve MSI
0f3f0161d3ff01bfd91f5036739491a2d8ab4f77a0a79b91a6894e5b09f1cfaf - LogMeIn/Goto Resolve MSI
638eb89f417e5416fedb8a0e62c6ba79f8a0b0d7ea8a427df9e367c7de61bc25 - LogMeIn/Goto Resolve MSI
4b6a8b86d9245cf775b4e80a6ac134efc8dfe0d673951671547d5894fb9be677 - LogMeIn/Goto Resolve MSI
f922eab1cce0bfb9aded5a862790faeafadd731e209b5b5f0358abb21db8fae - LogMeIn/Goto Resolve MSI
b9fcae4569904debd22d62773a1129350cf208d6c5f10289acc58ec9d6b95ba9 - LogMeIn/Goto Resolve MSI
1a0389d3631981a365bfa88ca38d5652cdf809d9155b6898c9734c2191f58bd1 - LogMeIn/Goto Resolve MSI
2c2f8a174c26f3c5c1974864d064eef1775f33c7c99963807925476cc6a06e50 - LogMeIn/Goto Resolve MSI
f625bb9827cfd17dccf5aebec2ffc13d32ae72fdd27c9c30f44090606c83343e - LogMeIn/Goto Resolve MSI
dfd99e2d876b486e1c49bd1b751b504e8a3dabdefdad9085fff915c0eeb133a7 - LogMeIn/Goto Resolve MSI
68e67f6b94c340ecd15e21eb2eca39e39c45f9b762b4bfaef7a4a1ad42ab7672 - LogMeIn/Goto Resolve MSI
57e40e729aa8e7d35398c4ea8d835996bb0d944b921317771cccd3350e02dd47 - LogMeIn/Goto Resolve MSI
a3c219bb005b9e66a254560d39e4f23f2cb4ad83d4290ebd31dbfd2d7e34e631 - LogMeIn/Goto Resolve MSI
98a988a199a0eccc518fc8a42641dfd7e733c378135041bbccada48b2d2b45ae - LogMeIn/Goto Resolve MSI
f52138d6a2878521f65c976086bd0376d231f073bfd4a28ab03a7e1ca88a487b - LogMeIn/Goto Resolve MSI
7b85a976ab6e787d28960989a124f7e74ed593782a2ccf7a9ce0713133683636 - LogMeIn/Goto Resolve MSI
0c2f38574675c37a10c9c6a57f7ff72e473c04541694d17113bc09d823486ff - LogMeIn/Goto Resolve MSI
3a4ef4b6f98b5b7644fad70fe3596b4f259b3ba4165c56ee178471d57e5ff565 - LogMeIn/Goto Resolve MSI
9b40976d3b04f8631bc7f981cd7a80c0dad5d2ffe5c3655a3c56bc6281625ba - LogMeIn/Goto Resolve MSI
d99c5cb3d217747a9a5ca87895a629819028880a92555f13628a3531498ca8bf - LogMeIn/Goto Resolve MSI
b7ac8c7c78b07575121d3f601423f85cc2a0f3b4ffff3df596a615d55a18298a - LogMeIn/Goto Resolve MSI
209d89d9c9b50f2b3d3c80dde98682c51a87afb505713a4a5792e3f499f6c385 - LogMeIn/Goto Resolve MSI
257f7f52e875e7525299e8d04d7f30f1a08cec3dbe5ebb4a01098ce427a4aefc - LogMeIn/Goto Resolve MSI
cc9ba2d8b999bec5da6b4b99bf8e64b8475fa3ad7192ada1b682e11dcd2af50d - LogMeIn/Goto Resolve MSI
745cc1b7f07d3544ab97678081e95f6c726783ed7f3cecdc00587a41966b5cb4 - LogMeIn/Goto Resolve MSI
0172d6646a87d42740b896d401f3c7d42ee88ee840e4413ee9b932fa72a9cbe3 - LogMeIn/Goto Resolve MSI
a7d9054cdfb653aa336a513fadb27905696b06fc68de1cf0749b301d31fba87e - LogMeIn/Goto Resolve MSI
2533ca461c55c6f2b34d6ec3e46a2378c2b1877616d19c677589e10b76b46869 - LogMeIn/Goto Resolve MSI
hxxps://cwwgg-p5wdxtar[.]com
hxxps://pishbinifoori[.]com/
hxxps://sas-govservice[.]com/
hxxps://sexydollies[.]com

hxxp://soraxpertai[.]com

hxxp://brukfield[.]com/eStatement-2025[.]msi

hxxp://luizmatoso[.]com[.]br/scr/omgo/Approval3546[.]msi?
redirect_mongo_id=6901fc3a62194ca8120dce2a&utm_source=Springbot&utm_medium=Email&utm_campaign=6901fc3a62194ca8120dce2b

hxxps://adobe[.]japsalgida[.]com/files/Acrobat_Reader_V112[.]msi

hxxps://artichaud[.]brussels/docusign/Docusign_em_ECOBenchtops_installer[.]msi

hxxps://file-na-phx-1[.]gofile[.]io/download/direct/f4842622-b8e3-477f-b3f9-2e8092717eb3/AdobeReader[.]msi

hxxps://gitlab[.]com/rockefellerroberth-stack/ui/-/raw/main/Dec_holidayparty[.]msi

hxxps://incandescent-lollipop-8c20fc[.]netlify[.]app/files/Adobe_Reader_v12[.]9332521[.]msi

hxxps://invitation-umber-one[.]vercel[.]app/success[.]html

hxxps://invoicepyament[.]vercel[.]app/success[.]html

hxxps://luizmatoso[.]com[.]br/scr/omgo/Approval3546[.]msi?
redirect_mongo_id=6901fc3a62194ca8120dce2a&utm_source=Springbot&utm_medium=Email&utm_campaign=6901fc3a62194ca8120dce2b/

hxxps://neuro-critical[.]com/s/OCTOMBER_SSA_statement[.]msi

hxxps://pub-0aa96c02ed4e4bc7a8792316381b1395[.]r2[.]dev/RSVP_INVITATION[.]msi

hxxps://pub-13fba6d38a5246708298bffda853443a[.]r2[.]dev/PARTY%20INVITE[.]msi

hxxps://pub-3986d29b7d784cb39f5a7cd218c1026d[.]r2[.]dev/RSVP_INVITATION_LIST[.]msi

hxxps://pub-6e736ff8b53e4bcfaafd02026051f756[.]r2[.]dev/PARTY%20INVITATION[.]msi

hxxps://pub-770ba80aa96043f098cb98f6ce8b415f[.]r2[.]dev/SPECIAL%20INVITE[.]msi

hxxps://pub-a0ee9b55473a4bfc6868499b2c995b9[.]r2[.]dev/special%20invitation[.]013[.]msi

hxxps://pub-d0a63a1c278246a7bd42edfc4ade9a1a[.]r2[.]dev/SPECIAL%20INVITATION%20(2)[.]msi

hxxps://pub-e079401ff51b491a872572ce873707c8[.]r2[.]dev/Download2025statement[.]msi

hxxps://pub-e63a077448d34769b25e250ef5a7c938[.]r2[.]dev/RSVP_ANNIVERSARY_2025[.]msi

hxxps://store3[.]gofile[.]io/download/direct/7cc1dc51-f000-42f1-abbd-7729f2e892ec/AdobeAcrobatReader[.]msi

hxxps://store3[.]gofile[.]io/download/direct/f4842622-b8e3-477f-b3f9-2e8092717eb3/AdobeReader[.]msi

hxxps://www[.]jfentradas[.]pt/maps/Receipt63MD2[.]msi

hxxps://gitlab[.]com/rockefellerroberth-stack/ui/-/raw/main/Dec_holidayparty[.]msi

hxxps://invoicepyament[.]vercel[.]app/success[.]html

hxxps://pub-75c6d59805624600bf89428e2354f7f3[.]r2[.]dev/BE%20MY%20GUEST[.]msi

hxxps://www[.]jfentradas[.]pt/maps/Receipt63MD2[.]msi

hxxp://transformedhost[.]com/Invoicepayment438990490903[.]exe

hxxp://www[.]otoaydinlatma[.]com[.]tr/RE2837464[.]msi

hxxps://cold-na-phx-8[.]gofile[.]io/download/direct/427b2109-99bc-46ca-9932-8e3b490a183f/Invitation_e-Card[.]exe

hxxps://drevos[.]ro/Re45766712[.]msi

hxxps://file-eu-par-1[.]gofile[.]io/download/direct/7bd9b6b2-ebc8-4b67-a59c-168ead5f6843/REVISED%20CONTRACT%20PROPOSAL[.]exe

hxxps://otoaydinlatma[.]com[.]tr/RE2837464[.]msi

hxxps://pcway[.]pt/bid/232invite_s_8DDFF00C56FF12-3-0_c_w[.]exe

hxxps://pub-cf31a0787efb46aa9b06228ed4f30934[.]r2[.]dev/SelectiveInvite[.]exe

hxxps://pub-d301f43b7bd442dfa91f65b23c225b3a[.]r2[.]dev/INVITATION_RSVP[.]msi

hxxps://pub-d78b53501c9a4b139654ec6601595157[.]r2[.]dev/Adobe_standalone_0[.]7[.]556[.]2[.]98[.]exe

hxxps://sdh[.]ro/Receiptv26394348[.]msi

hxxps://store-na-phx-1[.]gofile[.]io/download/direct/7bd9b6b2-ebc8-4b67-a59c-168ead5f6843/REVISED%20CONTRACT%20PROPOSAL[.]exe

hxxps://store-na-phx-2[.]gofile[.]io/download/direct/427b2109-99bc-46ca-9932-8e3b490a183f/Invitation_e-Card[.]exe

hxxps://store8[.]gofile[.]io/download/direct/32b65ce1-b844-41e9-a837-dbad055728c5/MsTeamSetup[.]exe

hxxps://store8[.]gofile[.]io/download/direct/fa290c5d-e61e-4e64-8c0e-2347945edef0/MSTeamssetup[.]exe

hxxps://transformedhost[.]com/Invoicepayment438990490903[.]exe

hxxps://uc00bab72c0d98ed6eeb52758dd3[.]dl[.]dropboxusercontent[.]com/cd/0/get/C0qFKHs00OpCJlcUzpw8cl0WOTJwR4i_KH2PFc5VoBYvnOzt7LTtD;dl=1

hxxps://ucb77371609cd949f38c83696b38[.]dl[.]dropboxusercontent[.]com/cd/0/get/C0o8UgdTzwr6QyiQw1oommfZ5S1XGF7ms2_Qj-qzRF10RlePfz_iQR6FamH-MF6PvqSAsFkoHzXJyaoslcoTzDUZ7MctvQHx0Csi1v1zOQmJ5SYBWLt1BCU6BsAlOL1AB5Cx31vih5Sn7R8EF_Qxd-B/file?dl=1

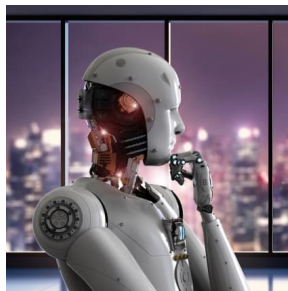
hxxps://vizyonuniversitesi[.]web[.]tr/Ref62535[.]msi

hxxps://www[.]dropbox[.]com/scl/fi/3jk5gxicsilax5vtlnqau/Or-amento-at-o-dia-20-do-10[.]?[.]exe?rlkey=jzapaziu3tlpmzrqc6qiorwqa&st=8jcbwop2&dl=1

hxxps://www[.]dropbox[.]com/scl/fi/usi4e5wgs9vf0y656j88/Resolve-Comprovativo-392-35-[.]pdf[.]exe?rlkey=i037oc7pfn9fy2qitpr6m1xad&st=1s6ywwvm&dl=1

hxxps://www[.]jifentradas[.]pt/maps/lnv34566[.]msi?redirect_mongo_id=690b675662194c435a0dce55&utm_source=Springbot&utm_medium=Email&utm_campaign=690b675662194c435a0dce56

About the Author



Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.