

A Sting on Bing: Bumblebee delivered through Bing SEO poisoning campaign

 cyjax.com/resources/blog/a-sting-on-bing-bumblebee-delivered-through-bing-seo-poisoning-campaign/

19 May 2025

Introduction

Bumblebee is a downloader malware which has become known for its sophistication and effectiveness. The malware [was first discovered in 2022](#) and was believed to be a tool for ransomware groups due to the developer's close ties with Conti. Since then, it has been used in various attacks and has been delivered through multiple methods, including phishing emails, malicious documents, and SEO poisoning.

Cyjax has identified one such campaign which used a series of fake download sites to target users of the Bing web browser. This report will explore how the campaign operates and the developments of this specific attack.

Update – 27.05.2025

Additional samples of the Bumblebee loader have been identified targeting software packages. As with the previously identified campaign, generic template sites were used when users directly visited the pages. The sole purpose of the pages appears to be generating SEO. However, when users visit these sites via a Bing referrer link, cloned download sites delivering the Trojanised MSI files are loaded.

Two new template sites have been identified, one of which is titled “*Arcanetvoa*”. The second template site appears to be entirely built from bootstrap style elements. Both can be viewed in **Figure U1 and Figure U2**.



Figure U1 – Arcanetvoa template site.



Download Wisenet Device Manager

The Wisenet Device Manager also lets the user create groups, generate reports, and configure key camera configurations. Live video can be previewed, PTZ positions configured, bulk focus cameras, and even save device configurations/templates to maximize programming capabilities on large installations.

[Write to us](#)

Wisenet Device Manager Latest Version by Hanwha Vision



Figure U2 – Second template site

The site shown in **Figure U2** has been linked to three targeted software packages, namely Sonicwall, Hanwhavision, and PulseSecure. Other identified phishing sites include downloads for Wireless Network Watcher, ZenMap, and Netcrunch. Each of these use a similar process to the previously identified campaign, leveraging a third-party site to deliver the malicious MSI file.

Through wider investigation, Cyjax has identified two new download sites named hub28[.]shop and vpncorporate[.]online. Both of these are hosted on the Hostinger IP address 157.173.208[.]204, the same server the previously identified download site was hosted on. From analysing publicly available DNS records, a number of other '.shop' and '.online' domains resolve to this IP. However, Cyjax has not directly linked these to Bumblebee campaigns.

Closer analysis of the infection chain showed that when downloading the Wisenet_Device_Manager.msi file hosted on the fake Hanwhavision site, it followed the exact execution pattern as WinMTR. The only difference is the use of a new version.dll file, which has the filename "*Periwinkled electrohemostasis*". As with the previous example, random words were used for the file information.

These sites highlight the targeting of a wider range of software packages to deliver Bumblebee. This is further evidenced by the sophistication of the attack, with an additional six software packages identified as targets. Consequently, this Bumblebee campaign is significantly wider reaching than initially thought. It is also clear that by targeting Sonicwall and Pulsesecure, the responsible threat actor is looking to target corporate software alongside lesser-known technical tools. As such, it is vital that those using the Bing web browser remain vigilant and ensure that all software download sites are verified through a third-party browser or source.

Update – Indicators of Compromise

Phishing Sites:

hanwhavision[.]org

pulsesecure[.]pro

sonicwall[.]pro

nir-soft[.]org

netcrunch[.]org

zenmap[.]pro

Download Sites:

hub28[.]shop

vpncorporate[.]online

Bumblebee C2 Domains:

7oo4hxt5haih5[.]life

9vgvnzk51j1sy[.]life

kks80hyrpbmuz[.]life

wi88w99xo9zlt[.]life

zom3rkt078g1k[.]life

New version.dll

18689fd0311a64a712a313d58fccbbfe

c135d29186faa04602d90e96d17aaf58fe16b8f7

a09923899b318848d44dc706ccc1d3489a383b9af0921351134d14a152a7925b

Wisenet_Device_Manager.msi

0a3439178f1cde7c5cfbeccee1a98a4a

- 7cdebee42a01b30f83e7770ca5154de4515d8245
- 5a847ecc862ee74dd532fef3a1e01c9f637631692fe74024b7ba15176cd9d13

Originally posted on – 19.05.2025

Technical Analysis

Within this newly identified campaign, Bumblebee has been delivered through a series of fake download websites for software packages. Currently, two packages called WinMTR and Milestone XProtect have been identified as targets of the attack. WinMTR is an open-source tool which provides a visual interface to a version of Matt's traceroute. This is a program which combines the functions of traceroute and ping. Milestone XProtect is a video management software which allows centralised control of video surveillance systems. In both cases, the threat actor created legitimate appearing sites to host the malicious downloader and registered domains which were similar to the original one. This can be seen in the table in **Figure 1**.

Legitimate Domain	Malicious Domain
www.milestonesys[.]com	www.milestonesys[.]org
www.winmtr[.]net	www.winmtr[.]org

Figure 1 – Domain typosquatting examples.

This specific campaign appears to target users of the Bing search engine, relying on SEO poisoning techniques to get malicious sites to the top of the search results. As can be seen in **Figure 2** and **Figure 3**, searches for “WinMTR download” and “Milestone XProtect download” show that the malicious sites appear as the top result below the panel generated by Bing.

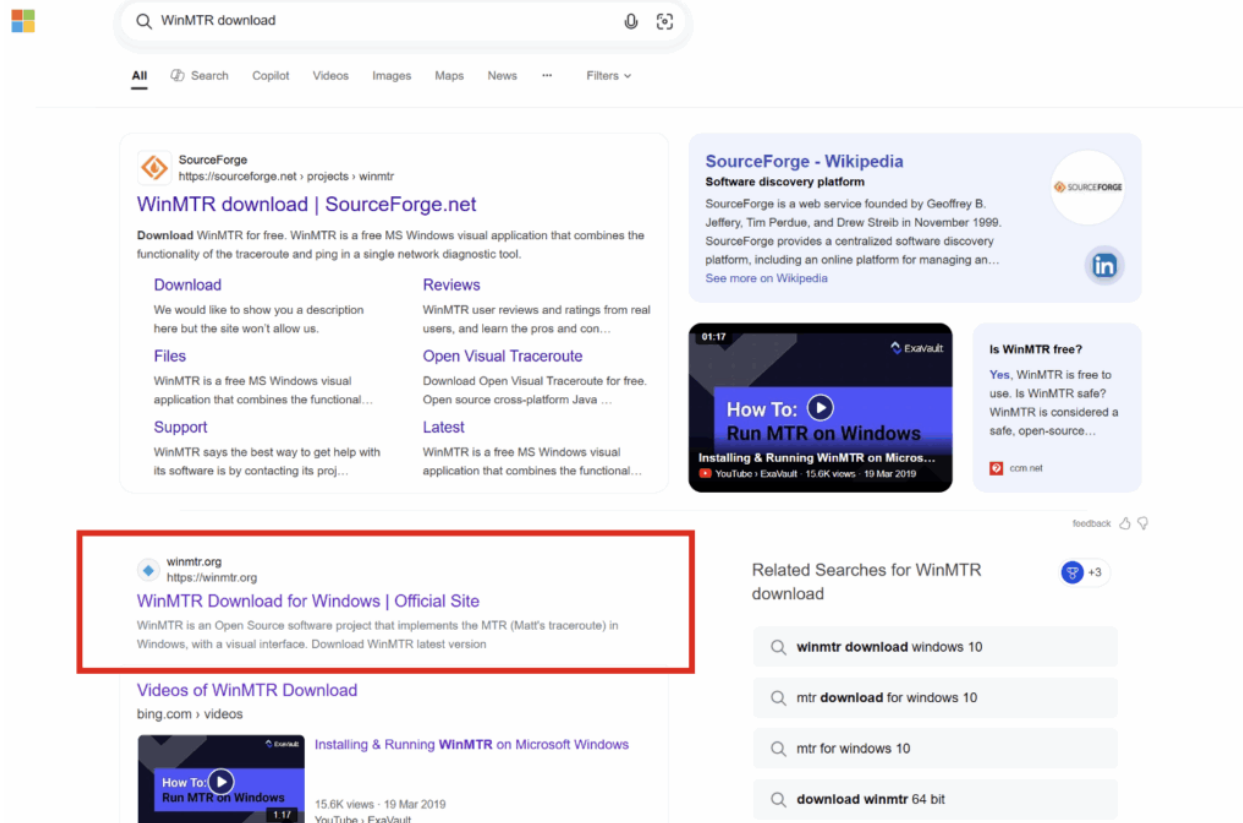


Figure 2 – “WinMTR download” search.

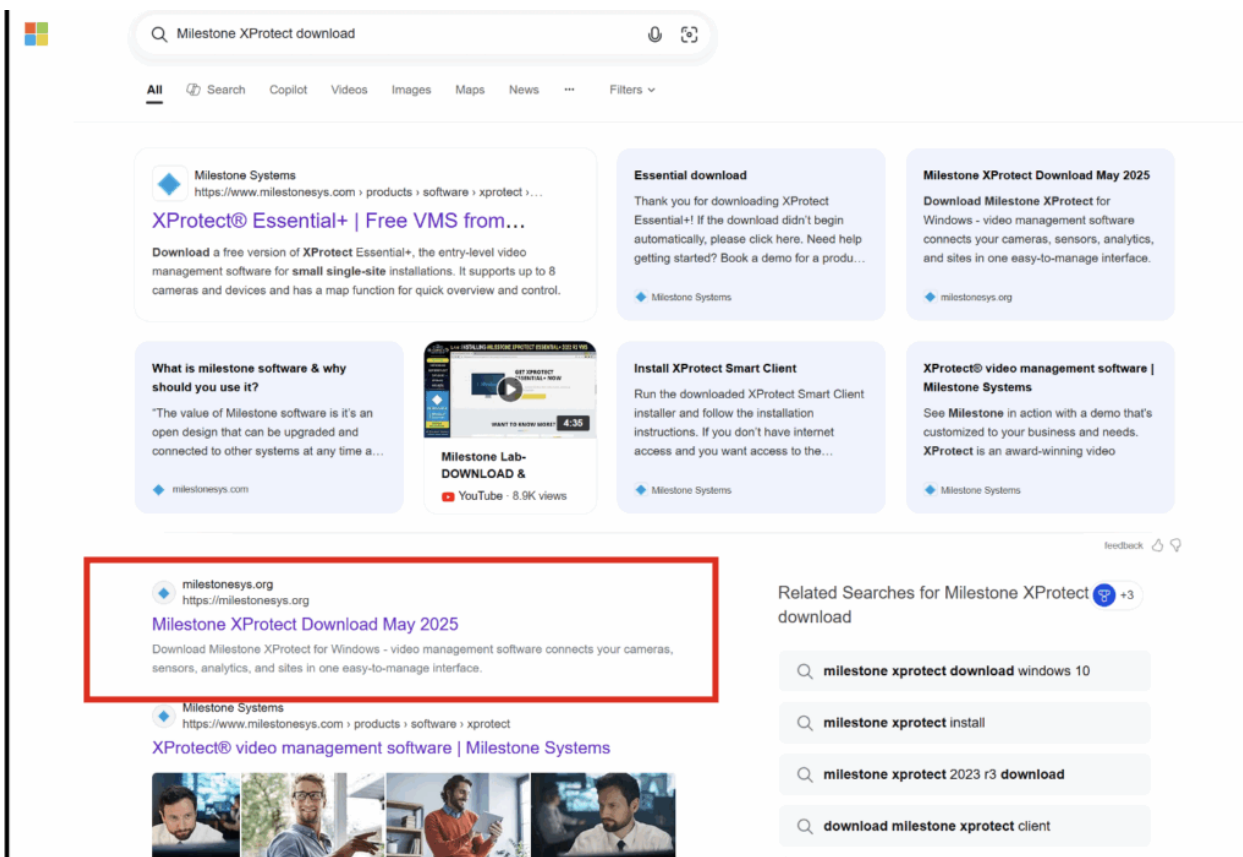


Figure 3 – “Milestone XProtect download” search.

Both sites are hosted on the same server owned by Truehost Cloud in Nairobi. Going directly to both sites load what appears to be a template website, with a number of assets and links still redirecting to the service “*LDAP Administrator*”.

LDAP Administrator

Company

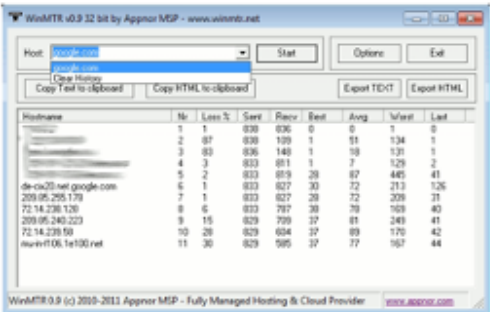
Download WinMTR for Windows



In an ever-evolving world, where security is paramount, WinMTR stands out as a leading video management software (VMS) that redefines the landscape of surveillance and security management. Designed for flexibility and scalability, XProtect caters to a diverse range of industries, from retail and transportation to critical infrastructure and public safety. Its robust features and intuitive interface empower users to manage their security operations with unparalleled efficiency and effectiveness..

At its core, WinMTR by provides real-time analysis of network paths, allowing users to trace the route packets take from their computer to a specified destination. By displaying each hop along the way, along with essential metrics such as packet loss and latency, WinMTR empowers users to identify potential bottlenecks and connectivity issues. This information is invaluable for both casual users seeking to enhance their internet experience and IT professionals tasked with maintaining robust network infrastructures.

One of the standout features of WinMTR is its ability to monitor network performance continuously. Users can initiate a test and watch as the program gathers data over time, presenting it in a clear and concise format. This ongoing analysis helps in pinpointing intermittent issues that may not be evident during a single test run. With options to export results for further examination or sharing with technical support teams, WinMTR becomes an indispensable ally in troubleshooting.



WinMTR v0.9.32 bit by Appnir MGP - www.winmtr.net

Hostname	No.	Loss %	Sent	Recv	Best	Avg	Worst	Last
1	1		830	830	0	0	1	0
2	87		830	109	1	11	134	1
3	93		836	140	1	18	131	1
4	3		833	811	1	7	129	2
5	2		833	819	28	87	445	41
6	1		833	827	33	72	213	126
de-cx20.net.google.com	7	1	833	827	38	72	209	71
209.85.205.179	8	6	833	787	38	79	169	40
72.14.238.126	9	15	829	709	17	81	243	41
209.85.240.223	10	28	829	634	17	89	170	42
72.14.238.59	11	30	829	585	17	77	167	44
newrtr06.te100.net								

WinMTR 0.9 (c) 2010-2013 Appnir MGP - Fully Managed Hosting & Cloud Provider www.appnir.com

Moreover, the software's lightweight design ensures that it runs efficiently on various Windows systems without consuming excessive resources. Its compatibility with both IPv4 and IPv6 networks further enhances its versatility, making it suitable for modern network environments.

WinMTR also stands out for its simplicity. With just a few clicks, users can start diagnosing their network connections, regardless of their technical expertise. The intuitive layout displays critical information at a glance, ensuring that even those new to networking can understand the data presented.

Figure 4 –Page contents of winmtr[.]org.

As seen in **Figure 4**, it is likely that this template site is being used to generate SEO for the tool and as a vague cover, so the site does not become suspicious to visitors. When visiting the site through the link provided in the Bing search engine, the legitimate WinMTR download site is shown, as highlighted in **Figure 5**.

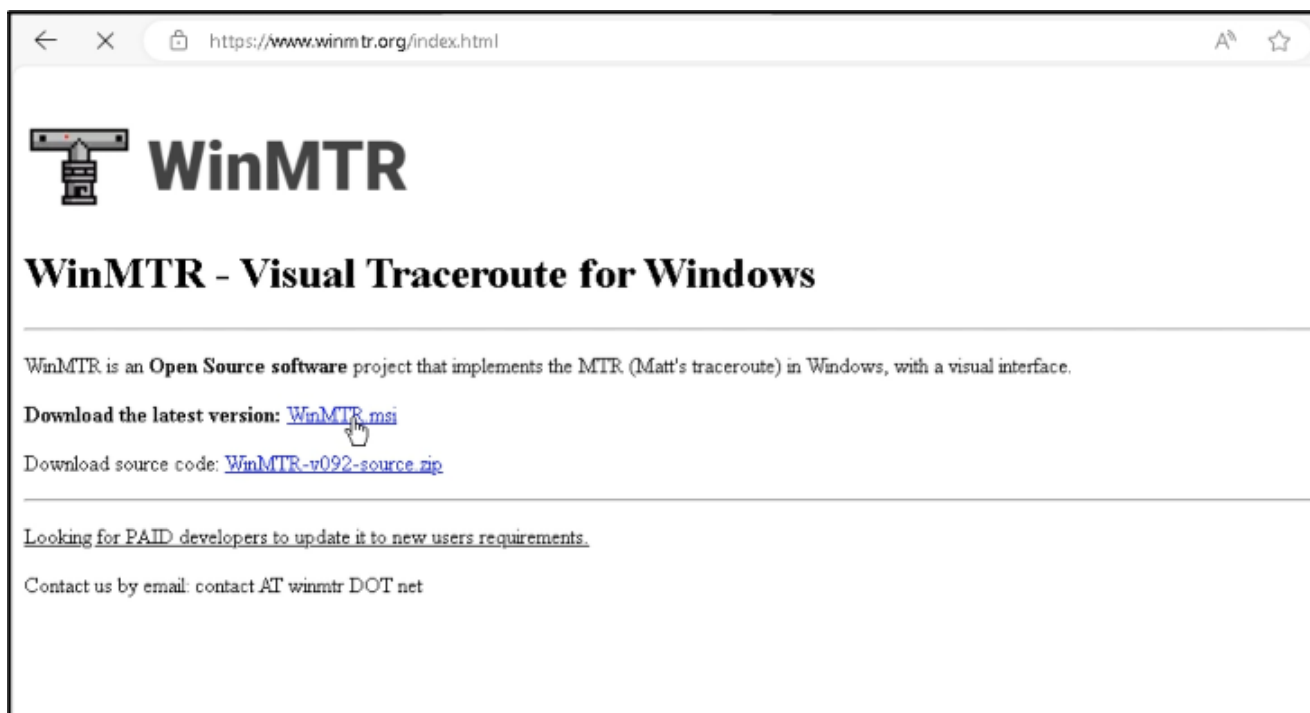


Figure 5 –Page contents of winmtr[.]org after visiting via Bing refer link.

The page is an exact copy, and the only change is that an MSI file is used for the latest version instead of a ZIP. This MSI file is the Trojanised installer which delivers the Bumblebee malware to victims once executed.

The file itself is not hosted locally on the same page. Instead, both sites reference an external domain called “*software-server[.]online*”, which hosts the malicious MSI files. A request is made to a page titled “*Get*” during download, with a parameter to specify which Trojanised software package to deliver. Currently, the two observed examples include WinMTR and Milestone_XProtect. However, this does suggest that there may be more available.

The installer is then installed using `msiexec.exe`, which delivers both the legitimate `winmtr.exe` executable, `icardagt.exe`, and a malicious DLL titled `version.dll`. Both the second executable and malicious DLL are responsible for delivering the malware, with `icardagt.exe` being used to load the malicious library. The executable appears to be a legitimate Windows binary; however, it is important to note that the certificate used to sign the executable expired on 22 January 2010. The breakdown of the execution flow can be seen below in **Figure 6**.

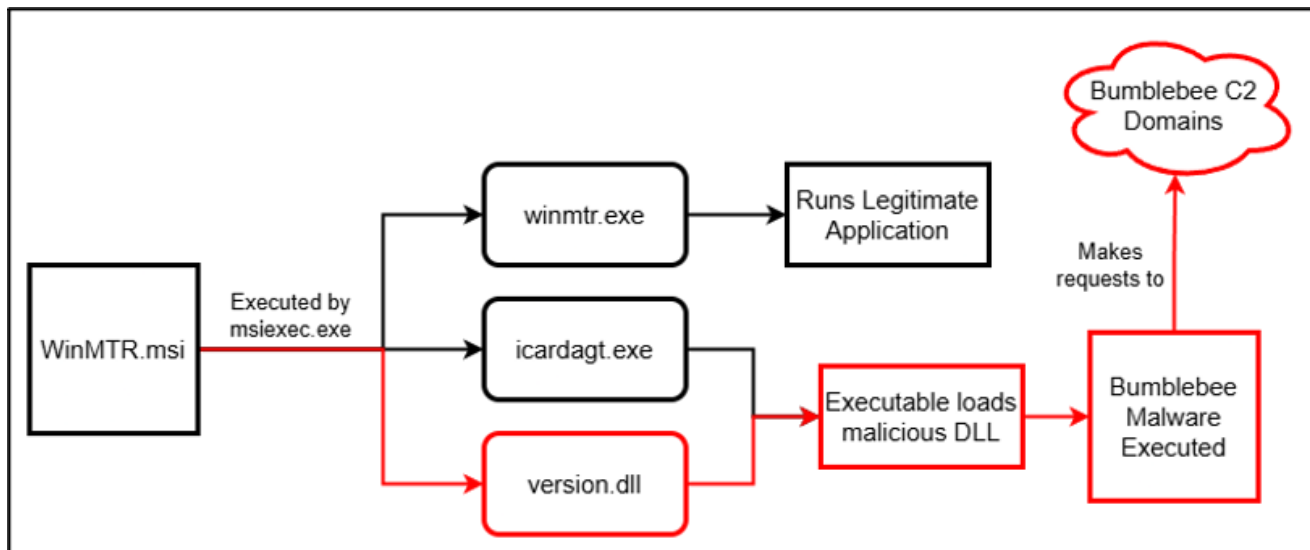


Figure 6 –Bumblebee execution flow.

After the malware is executed, it begins to connect to a number of known Bumblebee C2 domains. A series of C2 URLs have been identified, each taking the form of a 13-character string followed by the '.life' top-level domain (TLD).

These C2 domains have been linked to [a shared Bumblebee sample](#), in which a similar MSI file was delivered under the name RVTools.msi. This sample was also delivered through a similar delivery domain called “*soft-server[.]online*”, which is hosted on the same US-based server. This suggests that the threat actor responsible for this campaign has likely pivoted and further developed it to target more software packages through SEO poisoning.

Conclusions

Overall, this campaign highlights a clear targeting of software packages through a sophisticated and highly effective Bing SEO poisoning campaign. From analysing the software both across this and previous campaign, there is a common targeting of lesser-known tools used within technical development environments. This presents a unique target and because of Bumblebee’s ability to deliver additional malware, it is likely that these kind of privileged developer environments present an ideal environment for further attacks or information theft.

When comparing this to [a previous Bumblebee SEO poisoning campaign in 2023](#), the malware was delivered through Trojanised Zoom, Cisco AnyConnect, and ChatGPT installers. This new campaign highlights a significant shift in tactics, as the threat actor has pivoted to target more obscure software installation packages which victims may not easily be able to verify the legitimacy of.

The effectiveness of the SEO poisoning on Bing's search results highlights the importance of validating files before installing them. With both malicious packages appearing at the top, users cannot solely rely on search results ranking to provide legitimate software packages. It is because of this that users should regularly check other browsers or find a reputable third-party source to cross reference the legitimacy of the source.

Tactics Techniques and Procedures

Tactic	Technique	ID
Resource Development	Acquire Infrastructure: Domains	T1583.001
~	Stage Capabilities: SEO Poisoning	T1608.006
~	Stage Capabilities: Upload Malware	T1608.001
Initial Access	Drive-by Compromise	T1189
Execution	User Execution	T1204
~	User Execution: Malicious File	T1204.002
Defence Evasion	Masquerading	T1036
~	Masquerading: Match Legitimate Name or Location	T1036.005
~	System Binary Proxy: Msiexec	T1218.007
~	DLL Side-Loading	T1574.001

Indicators of Compromise

Phishing Sites:

- winmtr[.]org
- milestonesys[.]org

Download Site:

software-server[.]online

Bumblebee C2 Domains:

- 19ak90ckxyjxc[.]life
- o2u1xbm9xoq4p[.]life
- 9b10t4vyvx6b5[.]life
- 9nl2a1qma4swd[.]life

- gc9fctjq62t2e[.]life
- apsgw881ol7rs[.]life
- rmqa3jodwcmgd[.]life
- 85ur7zivhczam[.]life
- evzftxl2qjfj4[.]life
- cp2br7osw928r[.]life
- lhunevjdxw5kz[.]life
- jbrprj8im7aia[.]life
- rdg0u5n7237r5[.]life
- xwn7sukhzhbqv[.]life
- j34duklow92k3[.]life
- u8karkeeu2qtj[.]life
- 8vh7uizstjhn[.]life
- inkja7hekgcuv[.]life
- 8sg769rvpe1lp[.]life
- r4a4n001s7uhi[.]life
- r976ptnxbh52l[.]life
- tv9jc206cpnyd[.]life
- xf30997j6tp8z[.]life
- nl2jkkus8efp[.]life
- 5395dg0j4h79n[.]life
- oknzqkp6ph302[.]life
- v30ty639krk3p[.]life
- ey9n44bwtmjaw[.]life
- rlq13ng659buz[.]life
- 9vgvnzk51j1sy[.]life
- trtiqjiry7k05[.]life
- wi88w99xo9zlt[.]life
- 7oo4hxt5haih5[.]life
- hoieva2gl9tzx[.]life
- ey8axyn00x8sf[.]life
- kks80hyrpbmuz[.]life
- zom3rkt078g1k[.]life

version.dll

- a67fa1a060c07934c3de8612aaa0ebc2
- d1c5b38d3d91f925b16d616c1c9d3e05542f025d
- 96480ef5ccfa8fcb0646538c440103d97ab741ed83f4c2bcb7b4717569f88770

WinMTR.msi:

- 28c0caed1c9c242f60c8e0884ccbf976

- 0e6abeb79a84fc3e7683c5439607c8a17ef6ae77
- 31dd6d070a65a648b2be9ea2edc9efca26762c3875a8dde2d018eb064bc41e32

Milestone_XProtect.msi

- ea966dbfdd3f777727c827719e668f94
- 3437f8372c7d455085d24460147f27f6e2c009f5
- c6d5d2fff2cc422aca6dd5538f8351b8f2107a07a0df1f3ad8d69b050951ca1e

Receive our latest cyber intelligence insights delivered directly to your inbox

Simply complete the form to subscribe to our newsletter, ensuring you stay informed about the latest cyber intelligence insights and news.