Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Inside Secret Blizzard's Seven-Year Espionage Odyssey

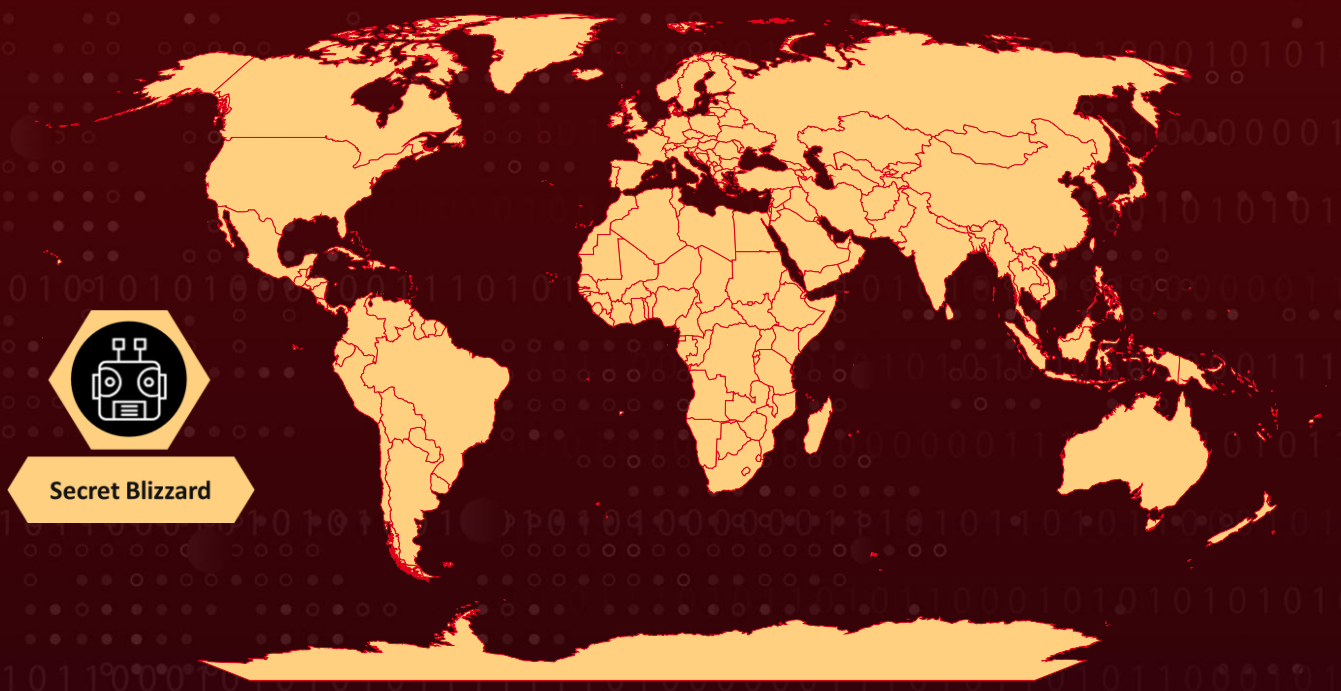
Date of Publication	Admiralty Code	TA Number
December 12, 2024	A1	TA2024461

Summary

Attack Commenced: 2017
Threat Actor: Secret Blizzard (aka Turla, Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard, Pensive Ursa, Blue Python)
Malware: TinyTurla, TwoDash, Wainscot, CrimsonRAT
Targeted Countries: Worldwide
Targeted Industries: Foreign Affairs, Embassies, Government, Defense, Military

Attack: Secret Blizzard, also known as Turla, is a Russian cyber-espionage group that has leveraged tools and infrastructure from at least six other threat actors over the past seven years. Renowned for maintaining long-term system access, they deploy advanced backdoors such as TwoDash and TinyTurla, frequently targeting politically sensitive intelligence and cutting-edge research. This innovative yet unconventional approach underscores their adaptability and resourcefulness in pursuing sophisticated espionage objectives.

Attack Regions



Attack Details

#1 Secret Blizzard, commonly identified as **Turla**, is a Russian cyber-espionage group renowned for its calculated use of tools and infrastructure utilized by at least six other threat actors over the past seven years. This tactic enables them to exploit environments already compromised by others, redirecting exfiltrated data to serve their intelligence-gathering agenda.

#2 Secret Blizzard's operations prioritize maintaining prolonged access to targeted systems, leveraging a sophisticated suite of tools. These include various backdoors featuring peer-to-peer capabilities and advanced command-and-control (C2) communication mechanisms.

#3 Their primary objective is to acquire politically sensitive intelligence, with a particular emphasis on cutting-edge research that holds potential geopolitical significance. In December 2022, Secret Blizzard infiltrated the infrastructure of Storm-0156, a threat cluster originating in Pakistan and linked to SideCopy, Transparent Tribe, and APT36.

#4 At first, they deployed a customized version of the TinyTurla backdoor on the C2 servers of Storm-0156. By October 2023, they had shifted to employing a .NET-based backdoor named TwoDash in conjunction with a clipboard monitoring utility known as Statuezy. This access granted them the ability to manipulate Storm-0156's backdoors, such as CrimsonRAT and Wainscot, while ensuring seamless communication with their proprietary C2 network.

#5 In 2017, Secret Blizzard utilized the tools and infrastructure of Hazel Sandstorm, an Iranian state-sponsored group also known as OilRig, APT-34, and Crambus. They employed the Andromeda malware to facilitate the deployment of their bespoke backdoors, KopiLuwak and QuietCanary, in 2022.

#6 Later, in 2022, Secret Blizzard capitalized on the backdoor associated with Storm-0473, a Kazakhstan-based adversary also known as Tomiris. This maneuver aimed to deploy their QuietCanary backdoor. While not entirely unprecedented, this approach underscores their resourcefulness and meticulous planning in pursuing intelligence-gathering objectives.

#7 Secret Blizzard's operations stand as a testament to their adaptability and ingenuity, exploiting the tools and vulnerabilities of other actors to advance their sophisticated espionage campaigns.

Recommendations

Strengthen Network Segmentation: Isolate sensitive systems and networks to limit lateral movement opportunities for advanced threat actors like Secret Blizzard.

Harden Endpoint Security: Enable application whitelisting and enforce strict controls on clipboard monitoring utilities to prevent unauthorized access by tools like Statuezy.

Enforce Application Whitelisting: Implement strict application whitelisting policies to prevent unauthorized or malicious executables from running within your environment.

Implement Zero Trust Principles: Adopt a Zero Trust architecture to enforce strict verification of all users and devices attempting to access network resources.

Enable Time-Based Access Control: Use time-based access restrictions for critical systems to prevent unauthorized access during non-working hours.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0040 Impact	TA0042 Resource Development	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1203 Exploitation for Client Execution	T1071 Application Layer Protocol	T1071.004 DNS

T1055 Process Injection	**T1036** Masquerading	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools
T1012 Query Registry	**T1082** System Information Discovery	**T1021** Remote Services	**T1021.001** Remote Desktop Protocol
T1078 Valid Accounts	**T1570** Lateral Tool Transfer	**T1005** Data from Local System	**T1105** Ingress Tool Transfer
T1583 Acquire Infrastructure	**T1560** Archive Collected Data	**T1584** Compromise Infrastructure	**T1584.004** Server
T1213 Data from Information Repositories	**T1587** Develop Capabilities	**T1587.001** Malware	**T1083** File and Directory Discovery
T1588 Obtain Capabilities	**T1588.002** Tool	**T1057** Process Discovery	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	146[.]70[.]158[.]90, 162[.]213[.]195[.]129, 146[.]70[.]81[.]81, 162[.]213[.]195[.]192, 154[.]53[.]42[.]194, 66[.]219[.]22[.]252, 66[.]219[.]22[.]102, 144[.]126[.]152[.]205, 185[.]229[.]119[.]60, 164[.]68[.]108[.]153, 209[.]126[.]6[.]227, 209[.]126[.]81[.]42, 209[.]126[.]7[.]8, 154[.]38[.]160[.]218, 144[.]126[.]154[.]84, 173[.]212[.]252[.]2, 185[.]213[.]27[.]94,

TYPE	VALUE
IPv4	167[.]86[.]113[.]241, 109[.]123[.]244[.]46, 23[.]88[.]26[.]187, 209[.]126[.]11[.]251, 173[.]249[.]7[.]111, 62[.]171[.]153[.]221, 149[.]102[.]140[.]36, 130[.]185[.]119[.]198, 144[.]91[.]72[.]17, 173[.]249[.]18[.]251, 176[.]57[.]184[.]97, 84[.]247[.]181[.]64, 38[.]242[.]219[.]13, 5[.]189[.]183[.]63, 38[.]242[.]211[.]87, 45[.]14[.]194[.]253, 173[.]212[.]206[.]227, 209[.]145[.]52[.]172, 185[.]217[.]125[.]195, 167[.]88[.]183[.]238, 143[.]198[.]73[.]108, 182[.]188[.]171[.]52, 94[.]177[.]198[.]94, 46[.]249[.]58[.]201, 95[.]111[.]229[.]253, 161[.]35[.]192[.]207, 91[.]234[.]33[.]48, 38[.]242[.]207[.]36, 167[.]86[.]118[.]69, 37[.]60[.]236[.]186
SHA256	e298b83891b192b8a2782e638e7f5601acf13bab2f619215ac68a0b61230a273, 08803510089c8832df3f6db57aded7bfd2d91745e7dd44985d4c9cb9bd5fd1d2, aba8b59281faa8c1c43a4ca7af075edd3e3516d3cef058a1f43b093177b8f83c, 7c4ef30bd1b5cb690d2603e33264768e3b42752660c79979a5db80816dfb2ad2, dbbf8108fd14478ae05d3a3a6aabc242bff6af6eb1e93cbead4f5a23c3587ced, 7c7fad6b9ecb1e770693a6c62e0cc4183f602b892823f4a451799376be915912, e2d033b324450e1cb7575fedfc784e66488e342631f059988a9a2fd6e006d381, c039ec6622393f9324cacbf8cfaba3b7a41fe6929812ce3bd5d79b0fdedc884a,

TYPE	VALUE
SHA256	59d7ec6ec97c6b958e00a3352d38dd13876fecdb2bb13a8541ab93248edde317
Domains	connectotels[.]net, hostelhotels[.]net

References

https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

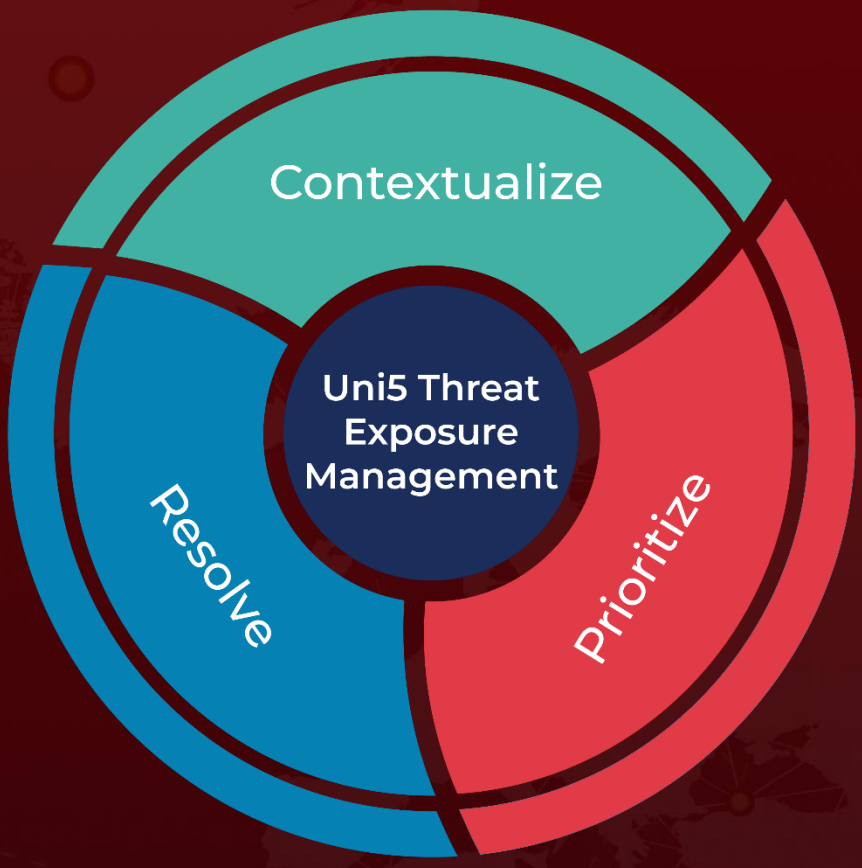
https://blog.lumen.com/snowblind-the-invisible-hand-of-secret-blizzard/

https://hivepro.com/threat-advisory/lunarweb-and-lunarmail-the-secret-weapons-of-the-turla-apt/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 12, 2024 . 3:00 AM

More at www.hivepro.com