Hive Pro

THREAT ADVISORY

Attacks on European Union and Ukrainian government entities carried out by the Armageddon group	TA2022090
Threat Level RED	**Publish Date –** April 12, 2022

The Computer Emergency Response Team of Ukraine (CERT-UA) has issued an alert warning of an ongoing spear-phishing attempt aimed at delivering an email with a malware attachment to Ukrainian government institutions and European state agencies. According to CERT-UA researchers, the hacker organization UAC-0010, also known as Armageddon, is responsible for spear-phishing attempts against Ukrainian government personnel.

The group's principal attack vector has been mass-sending emails to potential victims with harmful attachments that lead to the spread of different malware strains throughout the course of their exposed activity, and the most recent cyber-attacks are no exception. In the early days of their activity, the Gamaredon group used simple tools written in VBScript, VBA Script, C#, C++, and other programming languages, mostly relying on open-source software, before gradually expanding their toolkit with a number of custom cyber espionage tools, such as Pterodo/Pteranodon and EvilGnome malware.

The Mitre TTPs used by Armageddon are:
TA0001: Initial Access
TA0002: Execution
TA0005: Defense Evasion
T1566: Phishing
T1218: Signed Binary Proxy Execution
T1564: Hide Artifacts
T1059: Command and Scripting Interpreter

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
Armageddon (Gamaredon Group, Winterflounder, Primitive Bear, BlueAlpha, Blue Otso, Iron Tilden, SectorC08, Callisto, Shuckworm, Actinium, DEV-0157, UAC-0010)	Russia	Albania, Austria, Australia, Bangladesh, Brazil, Canada, Chile, China, Colombia, Croatia, Denmark, Georgia, Germany, Guatemala, Honduras, India, Indonesia, Iran, Israel, Italy, Japan, Kazakhstan, Latvia, Malaysia, Netherlands, Nigeria, Norway, Pakistan, Papua New Guinea, Poland, Portugal, Romania, Russia, South Africa, South Korea, Spain, Sweden, Turkey, UK, Ukraine, USA, Vietnam	Defense, Government, Law enforcement, NGOs and diplomats and journalists.	Information theft and espionage

Indicators of Compromise (IoCs)

Type	Value
SHA-256	69366a4e652041c78c2cc267288a4c4bb0d4eece4074adda82eecd11d9dcf08d, 945d49d58d2d3041aad9445487f01a13d863cf8e76151e9a5008615175f7e52e, 208fc38faf5a2267d837971b48889e855c0edc164c0b2edefff08d0782ccf1bb, 890f25ee7cfb2931536ee3e12fb75ce3f0be21ec03bdfdb38dc688db06e07198, de4040a631b95044e08797837e2143c64ef7c6b981547a9220f8ed7b40701ef9, b73314087130fe98896add3430787744de7310d3342b219bd668cdce79368f91, 596acbbfd7bc54dcc06123b7adfb7337f8ceab736004ce930d8286c8914b8e25, fa7bbc46a7b062a5828380b7c70a67cb47ba10c2ef127fd2348647313f65aa11, 7052cef3936c29707da0dd0d4696863b63971eefa1b0e7db611df2ce26b73f50, 8f429996f5be9d59d86ba4346de535a25b9a2c3e89cf2e29dbc053d13ae99269, ae3fabbbb2e2297e31435b7a57c486f0eaf0f01738da8d0ab68214dc92373666, cf7570cbbca779c755729484792208900a89564669785cb26e88442278ac52b2, 0b63f6e7621421de9968d46de243ef769a343b61597816615222387c45df80ae, 303abc6d8ab41cb00e3e7a2165ecc1e7fb4377ba46a9f4213a05f764567182e5, a0a39c06f56d63b9d37f7e72c24ec0768fe0aff497870ef879d7ae813d84bf1e, 09472d6bfb1c142a3b02f73175254a5e961f91e792dc9b347b099944bcfeab6f, 69366a4e652041c78c2cc267288a4c4bb0d4eece4074adda82eecd11d9dcf08d, 945d49d58d2d3041aad9445487f01a13d863cf8e76151e9a5008615175f7e52e, 208fc38faf5a2267d837971b48889e855c0edc164c0b2edefff08d0782ccf1bb, 890f25ee7cfb2931536ee3e12fb75ce3f0be21ec03bdfdb38dc688db06e07198, de4040a631b95044e08797837e2143c64ef7c6b981547a9220f8ed7b40701ef9, ad03c5f2add8c629f4294b2a7df440cbae213f466e18f98af66db0b82a4e4142, 452a89dd1c760881e0066a5f6c0fc7b5f936a90a197859a4f3ee74b39f705da0, ded51c96d161e9ac22782d7f9df37fe4816eae13be9369f9c8630ee706de53e1, baae0ac6b3873dfdec2587dcddfaf1a327aadf77f7fea6a1532960f31e3dd240
IPs	194 [.] 58,121,198 194 [.] 180,174,105 149 [.] 248.13.58 66 [.] 175,219,231 194 [.] 38.21.12 194 [.] 58.104.86
URLs	jokotras [.] ru tiloraso [.] ru milotrad [.] ru potrakit [.] ru tortunas [.] ru hxxp: // jokotras [.] ru / su / faicon.ico hxxp: // prefer [.] jokotras.ru/hear/nephew/su hxxp: // tiloraso [.] ru / get.php hxxp: // tiloraso [.] ru / index.php vadim_melnik88 @ i [.] ua hxxps: // military-ukraine [.] site / Necessary_military_assistance.rar hxxp: // military-ukraine [.] site / Assistance.rar hxxp: // military-ukraine [.] online / predicate / images / favicon.ico hxxp: // military-ukraine [.] online / headstone / images / favicon.ico hxxp: //co87972.tmweb [.] ru / select / guarded / favicon.ico hxxp: //co87972.tmweb [.] ru / intent / quick / favicon.ico hxxp: //co87972.tmweb [.] ru / seeing / network / favicon.ico military-ukraine [.] site

Type	Value
URLs	military-ukraine [.] online co87972.tmweb [.] ru hXXp: //m-vz.webhop [.] me / prk / faicon.ico hXXp: //a0656203.xsph [.] ru / prescription / seized.xml hXXp: //a0656203.xsph [.] ru / prepared / semi.xml m-vz.webhop [.] me a0656203.xsph [.] ru a0322810.xsph [.] ru webhop [.] me xsph [.] ru lnk-upload.dodortar [.] ru dod-upload.dodortar [.] ru ln-upl.ddns [.] no d-upl.ddns [.] no up-dot.myftp [.] org up-lnk.myftp [.] org nitikora [.] ru dodortar [.] ru kopratiso [.] ru billyhot [.] ru bilitora [.] ru

References

https://cert-gov-ua.translate.goog/article/39386?_x_tr_sl=uk&_x_tr_tl=en&_x_tr_hl=de&_x_tr_pto=wapp,
https://cert-gov-ua.translate.goog/article/39086?_x_tr_sl=uk&_x_tr_tl=en&_x_tr_hl=de&_x_tr_pto=wapp,
https://cert-gov-ua.translate.goog/article/39138?_x_tr_sl=uk&_x_tr_tl=en&_x_tr_hl=de&_x_tr_pto=wapp