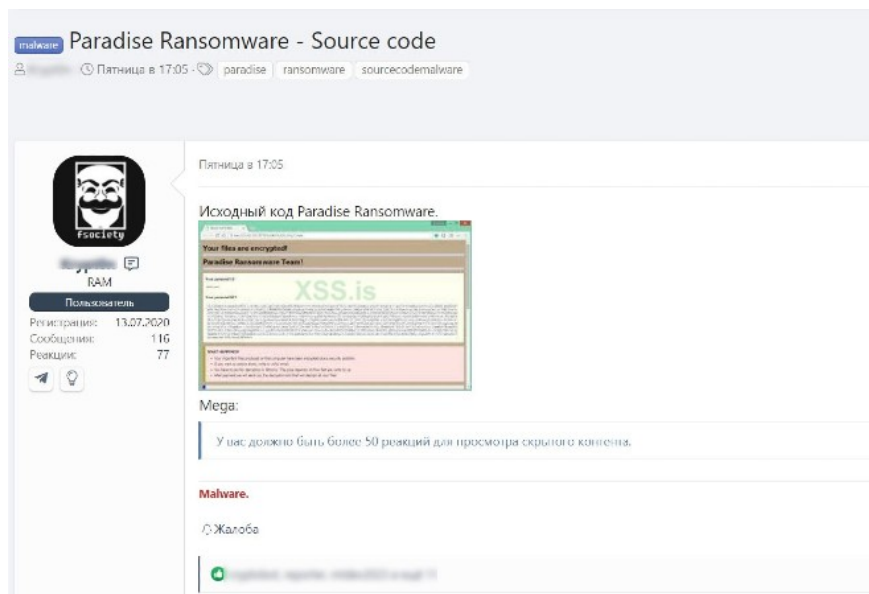


Paradise ransomware source code shared on hacker forum

The entire source code of the Paradise ransomware has been shared on a hacker forum called XSS.is. Based on this source code, even novice cybercriminals can create their own custom ransomware.

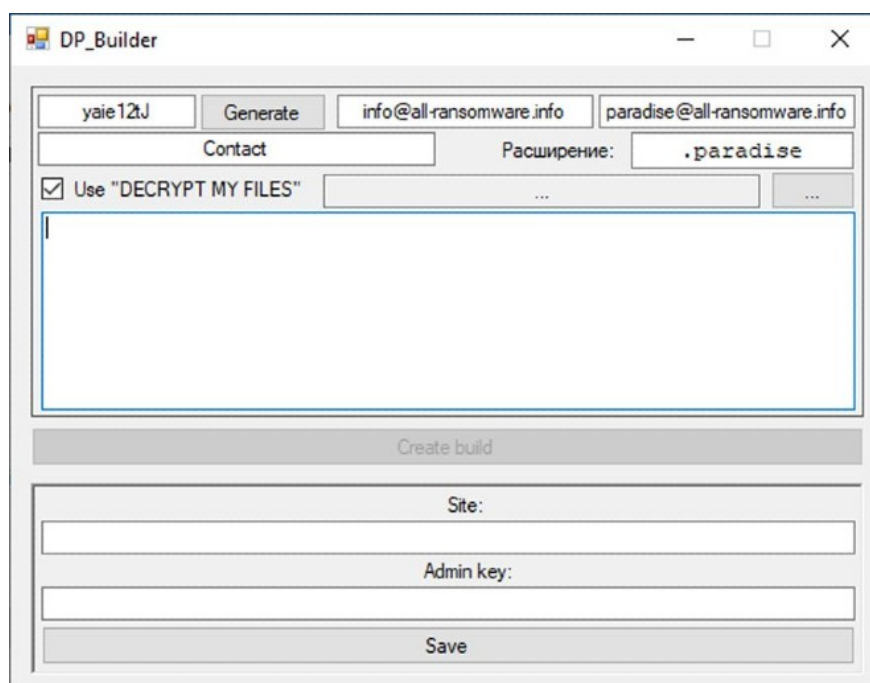
The Paradise source code is publicly shared, available for download by all active members of the XSS.is forum. XSS.is is a forum for hackers, mostly Russian hackers.



Security researcher Tom Malka downloaded the source code then compiled it and confirmed that it produces three executables. The first file is the ransomware configurator, the second is the encryptor, and the third is the decrypter.

```
Resources\cscx Notepad2
File Edit View Settings ?
657 [
658     public sealed class Program
659     {
660     const string name = "svch";
661     private static Thread[] Threads;
662     private object locker = new object();
663     private static string server = "%SERVER%";
664     private static string mail = "%FIRST_MAIL%";
665     private static string vector = "%INC_VECTOR%";
666     private static string text = "%TEXT FOR UNLOCK%";
667     private static string RSA_MasterPublic = "%RSA_PUBLIC%";
668     private static string CryptedExtension = "%EXTENSION%";
669     private static bool LockerForValidkey = true;
670     private static string PCID = "";
671     private static string RSA_Public = "";
672     private static string RSA_Private = "";
673     private static int FilesCount = 0;
674     private static bool SaveTextForUnlock = Boolean.Parse("%STFU%");
675     //private static bool SaveTextForUnlock = Boolean.Parse("true");
676     public static RSACryptoServiceProvider MasterRSA = new RSACryptoServiceProvider();
677     public static RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
678     public static List<string> directories = new List<string>();
679     private static string CryptedPrivatekey = "";
680     /// <summary>
681     /// Главная точка входа для приложения.
682     /// </summary>
683     [STAThread]
684     static void Main(string[] args)
685     {
686     try
687     {
688     var handle = NativeMethods.GetConsoleWindow();
689     NativeMethods.ShowWindow(handle, NativeMethods.SW_HIDE);
690     string appdata = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
691     }
692     }
693     }
694     }
695     }
696     }
697     }
698     }
699     }
700     }
701     }
702     }
703     }
704     }
705     }
706     }
707     }
708     }
709     }
710     }
711     }
712     }
713     }
714     }
715     }
716     }
717     }
718     }
719     }
720     }
721     }
722     }
723     }
724     }
725     }
726     }
727     }
728     }
729     }
730     }
731     }
732     }
733     }
734     }
735     }
736     }
737     }
738     }
739     }
740     }
741     }
742     }
743     }
744     }
745     }
746     }
747     }
748     }
749     }
750     }
751     }
752     }
753     }
754     }
755     }
756     }
757     }
758     }
759     }
760     }
761     }
762     }
763     }
764     }
765     }
766     }
767     }
768     }
769     }
770     }
771     }
772     }
773     }
774     }
775     }
776     }
777     }
778     }
779     }
780     }
781     }
782     }
783     }
784     }
785     }
786     }
787     }
788     }
789     }
790     }
791     }
792     }
793     }
794     }
795     }
796     }
797     }
798     }
799     }
800     }
801     }
802     }
803     }
804     }
805     }
806     }
807     }
808     }
809     }
810     }
811     }
812     }
813     }
814     }
815     }
816     }
817     }
818     }
819     }
820     }
821     }
822     }
823     }
824     }
825     }
826     }
827     }
828     }
829     }
830     }
831     }
832     }
833     }
834     }
835     }
836     }
837     }
838     }
839     }
840     }
841     }
842     }
843     }
844     }
845     }
846     }
847     }
848     }
849     }
850     }
851     }
852     }
853     }
854     }
855     }
856     }
857     }
858     }
859     }
860     }
861     }
862     }
863     }
864     }
865     }
866     }
867     }
868     }
869     }
870     }
871     }
872     }
873     }
874     }
875     }
876     }
877     }
878     }
879     }
880     }
881     }
882     }
883     }
884     }
885     }
886     }
887     }
888     }
889     }
890     }
891     }
892     }
893     }
894     }
895     }
896     }
897     }
898     }
899     }
900     }
901     }
902     }
903     }
904     }
905     }
906     }
907     }
908     }
909     }
910     }
911     }
912     }
913     }
914     }
915     }
916     }
917     }
918     }
919     }
920     }
921     }
922     }
923     }
924     }
925     }
926     }
927     }
928     }
929     }
930     }
931     }
932     }
933     }
934     }
935     }
936     }
937     }
938     }
939     }
940     }
941     }
942     }
943     }
944     }
945     }
946     }
947     }
948     }
949     }
950     }
951     }
952     }
953     }
954     }
955     }
956     }
957     }
958     }
959     }
960     }
961     }
962     }
963     }
964     }
965     }
966     }
967     }
968     }
969     }
970     }
971     }
972     }
973     }
974     }
975     }
976     }
977     }
978     }
979     }
980     }
981     }
982     }
983     }
984     }
985     }
986     }
987     }
988     }
989     }
990     }
991     }
992     }
993     }
994     }
995     }
996     }
997     }
998     }
999     }
1000    }
```

Scattered inside the source code are lines of comments in Russian. This shows that the author of this ransomware uses Russian.



Once they have the source code, hackers can create their own custom ransomware. Customizable sections include control server, encrypted extension file statement, and contact email address.

After the customization is complete, the hacker can deploy and distribute to the victim.

Welcome to Paradise

Ransomware Paradise first appeared in September 2017 through phishing emails containing malicious IQY attachments. Clicking on this file, the ransomware will be downloaded and installed on the victim's machine.

Over time, many versions of Paradise have been released because the first versions contained vulnerabilities that security experts could easily decipher. On the new versions, Paradise has used RSA encryption method, so it is much more difficult to decrypt.

According to Michael Gillespie, the creator of the decryptor for the first version of Paradise, the Paradise ransomware has the following versions:

1. Paradise - Original version with holes
2. Paradise .NET - .NET secure version switches to RSA encryption algorithm
3. Paradise B29 - A variant that only encrypts the end of the file

Ransomware Paradise, which was heavily distributed in the period from September 2017 to January 2020, suddenly reduced the frequency of terrorizing victims. Until now, it is very rare to see computers infected with this ransomware.

Maybe Paradise will return once the source code is shared publicly.

You finished reading the article "**Paradise ransomware source code shared on hacker forum**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.